

# Radia Client Automation Enterprise Application Usage Manager

For the Windows® operating systems

Software Version: 9.00

---

## Reference Guide

Document Release Date: April 2013

Software Release Date: June 2013



# Legal Notices

## Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Persistent Systems shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Valid license from Persistent Systems or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Persistent Systems.

## Copyright Notice

© Copyright 2013 Persistent Systems, its licensors, and Hewlett-Packard Development Company, LP.

## Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft®, Windows®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.

## Acknowledgements

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

This product includes software written by Daniel Stenberg ([daniel@haxx.se](mailto:daniel@haxx.se)).

This product includes OVAL language maintained by The MITRE Corporation ([oval@mitre.org](mailto:oval@mitre.org)).

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

**<http://support.persistentsys.com/>**

This site requires that you register for a Persistent Passport and sign in. Register online at the above address.

For more details, contact your Persistent sales representative.

# Support

Persistent Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Persistent support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-solve knowledge base, visit the [Persistent Support](#) home page.

**Note:** Most of the support areas require that you register as a Persistent Support user and sign in. Many also require an active support contract. More information about support access levels can be found on the [Persistent Support](#) site.

To register for a Persistent Support ID, go to: [Persistent Support Registration](#).

---

# Contents

Reference Guide .....	1
Contents .....	5
Introduction .....	10
Audience .....	10
Application Usage Manager .....	10
Data Collection Types .....	11
Abbreviations and Variables .....	12
Processing .....	12
Application Usage Manager Environment .....	12
Application Usage Manager Agent Operation Overview .....	13
Active Application Monitoring File .....	13
History File .....	14
Collection files .....	14
Collection Processing .....	15
Collection Point Destinations .....	15
Automated Import .....	15
Collection Destination Point Unavailable .....	16
Agent Processing of Data Collection Request .....	16
Executable Inventory Scan and Options .....	16
Initiating Collection of Agent Data .....	16
Portal Web Services and the Application Usage Manager .....	17
Configuring Your Environment .....	18
Database Performance and Maintenance .....	18
Using Standard Materialized Views and Filtered Materialized Views .....	18
Applying the Scripts for SMV or FMV: .....	18
Optional Utility Scripts .....	19
Miscellaneous Scripts for Oracle .....	19

Concept of Current Computer .....	19
Configuring the RCA Knowledge Base Server .....	20
Starting and Stopping the KB Server .....	23
SQL Server Requirements for the KB Server .....	23
<b>Aggregation of Usage Data Files with Tier-Level Store and Forward .....</b>	<b>24</b>
Introduction .....	24
Aggregation .....	24
Implementation .....	24
Configuring Usage Data Files Store and Forward .....	26
Configuring Aggregation .....	27
About the Sections in the USAGE.DDA.CFG File .....	27
Performance .....	29
<b>Application Usage Manager Agent .....</b>	<b>30</b>
The USAGE Domain Defined .....	30
Significance of Collection Instances .....	31
Configuring the Application Usage Manager Agent .....	31
Viewing Attribute Description and Name in the Application Class Instance Attributes ..	32
Configuring the Application Usage Manager Agent for Distribution .....	32
Filters .....	36
Criteria, Rule, and Set .....	36
Filter Criteria Class (UMFLTCRI) .....	37
Filter Rule Class (UMFLTRUL) .....	37
Filter Set Class (UMFLTSET) .....	37
Using Filters .....	38
Filter Set Class Instances .....	38
Applying Filters .....	38
Applying a Filter to a Collection Class .....	39
Creating Filters .....	39
Creating a Filter Criteria Instance .....	39
Creating the Filter Rule Instance .....	40
Creating the Filter Set Instance .....	41
Using Concurrency .....	41

Enabling Concurrency Usage Data Collection .....	42
Initiating Inventory and Usage Collections .....	42
Initiating Inventory Data Collection .....	42
Configuring Usage Data Collection .....	42
Defining a Database Collection Point .....	43
Initiating a Usage Data Collection Request .....	43
Initiating a Usage Data Re-collection Request .....	43
Enabling Privacy .....	44
Handling Renamed Device .....	45
Internet Explorer Usage Counts for Windows Vista .....	45
<b>Viewing Application Manager Usage Reports .....</b>	<b>46</b>
Viewing Usage Reports .....	46
Usage Reports .....	46
Executive Summaries .....	46
Monthly Device Collection Statistics .....	47
Daily Device Collection Statistics .....	47
Monthly Usage by Vendor .....	47
Monthly Usage by Product .....	47
Top 10 Used Products Reports .....	47
For User Accounts - Total Usage Time .....	47
For User Accounts - Total Focus Time .....	47
For User Accounts - Average Usage Per Day .....	47
For User Accounts - Average Usage Per Day For User Accounts .....	48
For Computer Accounts - Total Usage Time .....	48
For Computer Accounts - Total Focus Time .....	48
For Computer Accounts - Average Usage Per Day .....	48
For Computer Accounts - Average Usage Per Day For Computer Accounts .....	48
Operational Reports .....	48
Device Collected .....	48
Device Not Collected .....	49
Database Statistics .....	49
Device Reports .....	49

Usage by Device .....	49
Usage by User .....	49
Monthly Usage Reports .....	49
Vendor Reports .....	49
Monthly Usage by Vendor .....	49
Product Reports .....	50
Monthly Usage by Product .....	50
Monthly Usage by Product Version .....	50
Application Reports .....	50
Monthly Usage by Application .....	50
Monthly Usage by Application Version .....	50
Inventory Reports .....	51
Vendor Reports – Inventory by Vendor .....	51
Product Reports .....	51
Inventory by Product .....	51
Inventory by Product Version .....	51
Inventory by Application .....	51
Inventory by Application Version .....	52
Inventory by Application Signature .....	52
Filtering Usage Management Reports with Reporting Server .....	52
<b>Using the Application Usage Manager Administrator .....</b>	<b>54</b>
Accessing the Application Usage Manager Administrator .....	54
Application Usage Manager Admin Search Function .....	54
Creating Criteria, Rules, Rule Sets, and Rule Set Groups .....	54
Operators AND versus OR .....	55
Criteria Tab .....	55
Creating a criterion .....	57
Rules Tab .....	58
Creating a new Rule .....	59
Rule Sets Tab .....	59
Creating a new Rule Set .....	60
Rule Set Groups Tab .....	60



Creating a new Rule Set Group ..... 61

[We appreciate your feedback!](#) ..... 62

# Chapter 1

---

## Introduction

Application Usage Manager enables you to assess patterns of application usage in your environment. This enables you to facilitate adherence to license agreements, re-provision licenses if required, and monitor user productivity.

This chapter describes the Application Usage Manager processing and overview of Application Usage Manager agent.

## Audience

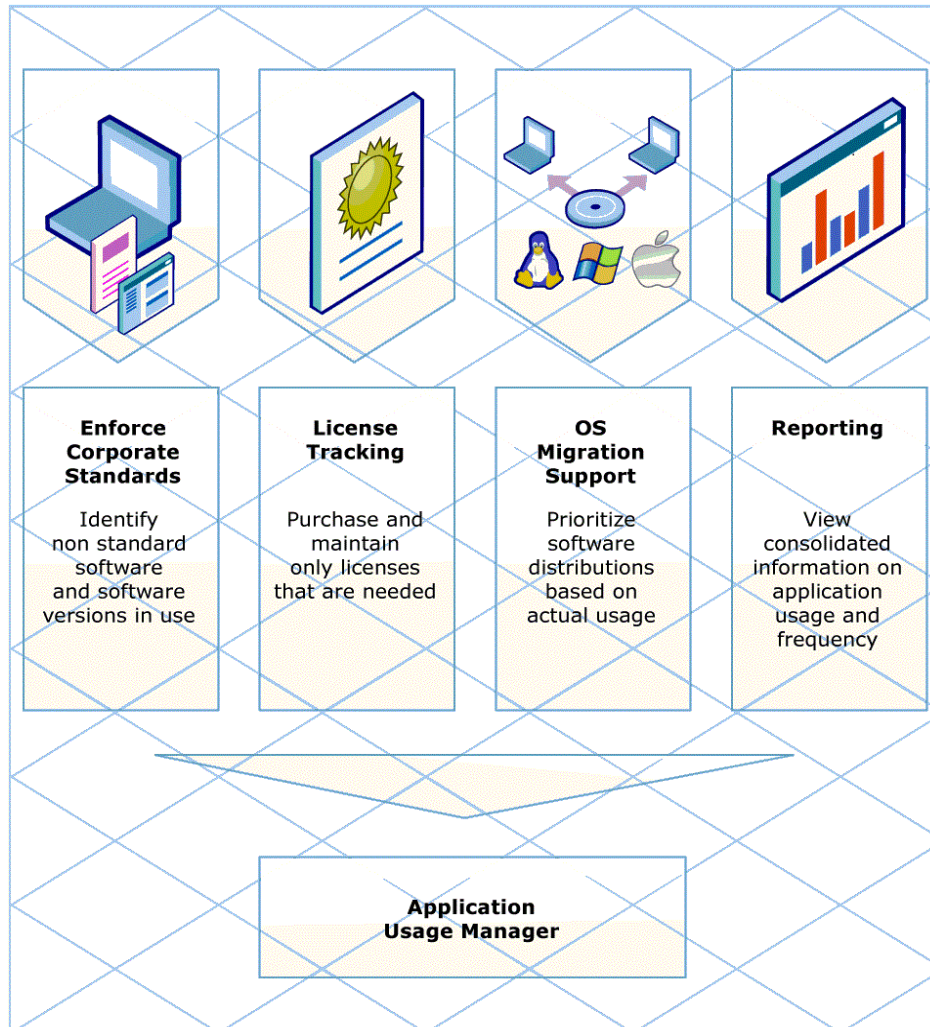
This guide is written for system administrators who want to use the Radia Client Automation Application Usage Manager (Application Usage Manager) to assess and obtain reports on software usage in their IT enterprises. The Application Usage Manager enables an administrator to know who is using what applications, and how often. Armed with this information, an administrator can increase efficiency by prioritizing and implementing IT projects, accordingly.

## Application Usage Manager

The Application Usage Manager monitors the use of every application on all of your servers, desktops, and laptops. This enables you to:

- Enforce corporate standards by identifying non-standard software and software versions in use within your enterprise.
- Implement license tracking, giving you the ability to purchase and maintain only those licenses that are required.
- Enable OS migration support by prioritizing software distribution based on actual usage.
- Use reporting to view the actual use of application resources.

## Application Usage Manager



## Data Collection Types

The Application Usage Manager collects two types of application data: usage and inventory.

- Inventory data consists of information about all applications currently installed on a computer.
- Usage data consists of information about what applications were in use over a specific time period.

Usage data incorporates another form of data called concurrency usage. Concurrency usage data is a more specific form of usage data.

Regular usage data is collected on a daily basis anytime an application is used during the course of a day, while concurrency data can be collected for a single application over a period of time as short as fifteen minutes. This ability enables for capacity planning as well as provides specific data to organizations that may be interested in migrating users into a terminal server environment.

## Abbreviations and Variables

### Abbreviations Used in this Guide

Abbreviation	Definition
RCA	Radia Client Automation
Core and Satellite	RCA Enterprise environment consisting of one Core server and one or more Satellite servers.
CSDB	Configuration Server Database

### Variables Used in this Guide

Variable	Description	Default Values
<i>InstallDir</i>	Location where the RCA server is installed	For a 32-bit OS: C:\Program Files\Hewlett-Packard\HPCA  For a 64-bit OS: C:\Program Files (x86)\Hewlett-Packard\HPCA
<i>SystemDrive</i>	Drive label for the drive where the RCA server is installed	C:

## Processing

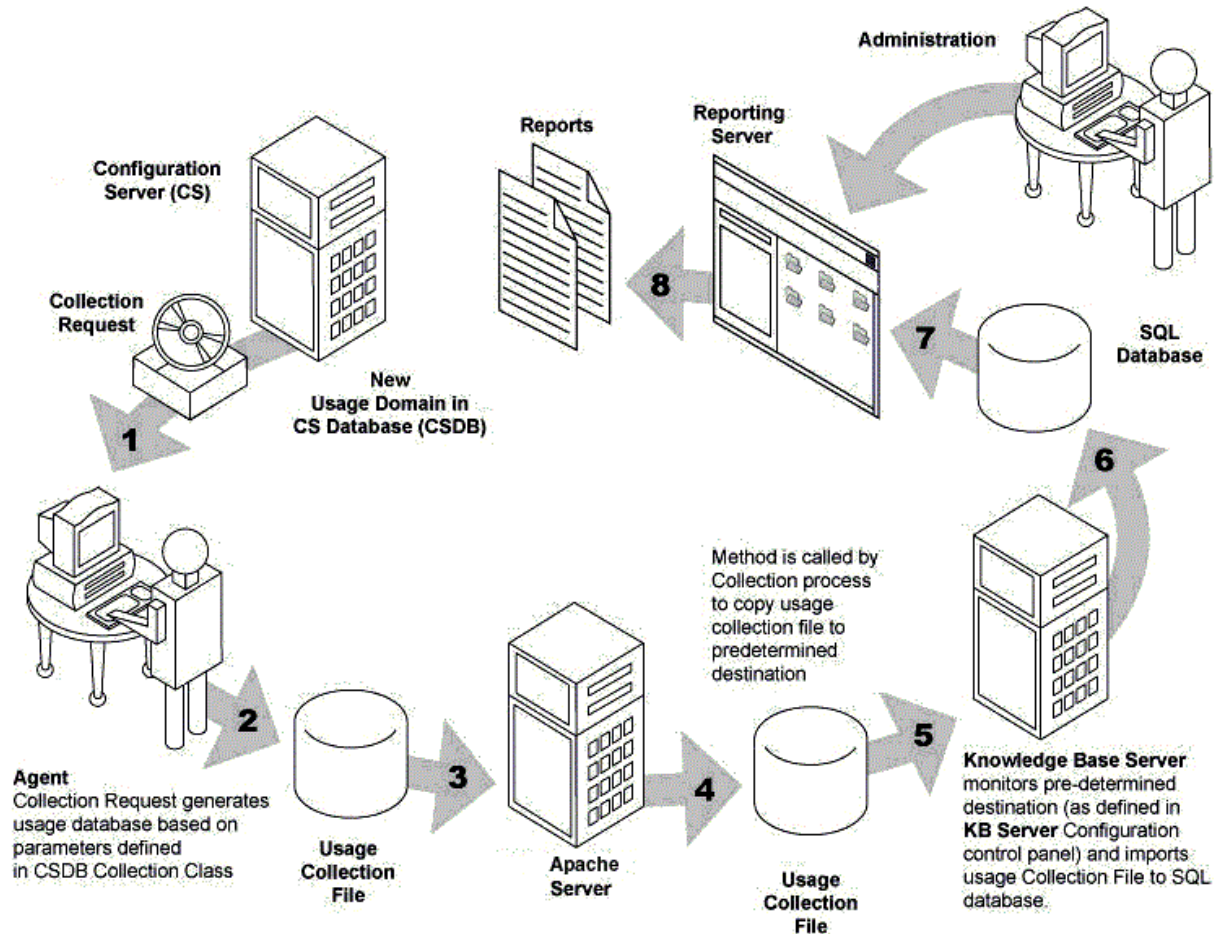
You can distribute and install the Application Usage Manager agent on your computers using your existing RCA infrastructure. Default RCA-defined installation settings install and configure the Application Usage Manager agent to perform executable inventory scanning, application usage, and usage data collection through predefined Application Usage Manager Packages. The next time an agent connects to the Configuration Server, the package is delivered and Application Usage monitoring begins automatically.

Periodically, the usage data is collected based on user-defined parameters. This data is sent to a predefined collection point for further processing. Collection points may be a network share or an RCA Portal destination. This location is monitored by the RCA Knowledge Base Server (KB Server), which in turn extracts the usage data from the files collected from each agent computer and loads this data into your SQL-enabled database, making the data available for reporting purposes. Reports are generated using the Reporting Server.

## Application Usage Manager Environment

The Application Usage Manager has different infrastructure requirements, based on whether or not RCA is being used to manage the environment.

## Application Usage Manager Environment



## Application Usage Manager Agent Operation Overview

The Application Usage Manager agent supports monitoring of all executable usage.

Once monitoring has started, there are three usage files on the agent machine: the active application monitoring file, the history file, and the collection file.

### Active Application Monitoring File

Contains current application usage information, including (where available):

- Machine name
- Machine domain name
- OS major, minor, build versions
- User name
- User domain name

- Vendor name
- Product name
- Product version
- Application name
- Application version
- Original application name (if renamed)
- Application description
- Application module file type
- Path name application was launched from
- Logical root folder name (ProgramFilesFolder)
- Remaining path name
- MD5 hash
- Link time
- Number of times application was launched
- Number of seconds application was active
- Number of seconds application was in the foreground or "in-focus"

## History File

- Data is accumulated in a history file by machine, user, executable, and day. Note that data is summarized by day in the history file.
- The usage history file is maintained for a designated period (default is the last 12 months).
- Old data is aged out of the file.
- The agent history file maintains separate entries for all executable inventory and usage data reported to each database.

## Collection files

- Contains the usage and current executable inventory data that is to be imported into a specific SQL Server or Oracle database. Data collection is done on a per database basis.
- Each database has a filter policy associated with it that contains a set of filtering rules. A collection file is built for each database.
- There can be any number of usage monitor databases that can request the same or different data from any agent based on the filtering rules.
- Filter policies are maintained for each database on the agent or as objects in the Configuration Server.

- The agent-generated collection file must be sent to the correct database import path. The KB Server imports the collection data file. The Portal performs the role of moving the collection files to the database import path location.
- When implemented through RCA, the default collection file name is the &ZOBJID of the UMCOLLCT Class.

## Collection Processing

When collection is requested for a database, the agent compares the current archive data against the reported data for that database. All file inventory data is compared. Usage data is only compared for files that pass the inclusion filter. Any differences in inventory or usage are added to the collection file.

Once the collection file has been created, it is sent to the destination defined in the PRIMARY.USAGE.UMDESTPT class, COLLDEST instance attribute.

To minimize bandwidth requirements, the collection files contain only what has not yet been sent to the specific database requesting the collection. These files also contain data aging and deletion information for removing old data from the database.

The history file contains all usage data, regardless if it has been requested for upload into a database for the machine and all of its users. The history file contains up to one year's data and as new days are added, data older than one year is deleted. The number of months is determined by the History Retention Months setting. This feature enables a database collection process to modify policy collection filters to capture any data that is up to a year old. If a new database is added as a destination point, then it can request any of this data from any machine that the Application Usage Manager has monitored—either presently or in the past.

## Collection Point Destinations

A collection point is a directory destination to which a collection file is copied, and then automatically imported into a SQL database by the KB Server.

## Automated Import

Automated import directories are watched by the KB Server automated import service. Automated importing can be defined for two types of directory structures:

- **Import Directories**  
These are state file automated import directories containing RCA state files (`.ISState` extensions). These are typically created by the Packager for Windows Installer.
- **Export Directories**  
These are Configuration Server Service export directories, which require subdirectory structures built by the Packager for Windows Installer. The Packager for Windows Installer features enables extraction and conversion of RCA packages contained in RCA Services to `.ISState` file formats.

**Note:** Any export directory must include a subdirectory named varsets.

The state file export process may only occur when the Configuration Server is active. However, the KB Server automated import server runs independently to import state files found in the automated import directories.

Each time a new collection file is placed in an auto-import directory, the files are identified by the KB Server. The KB Server then performs the following processing:

- Connect to its preconfigured SQL database through a system-level ODBC connection.
- Import the contents of the collection file into the SQL database.
- Archive the collection file once the import is successful, or copy it to an error directory should the import fail for any reason.
- Perform a rollback of the import if the import is unsuccessful.

## Collection Destination Point Unavailable

If a collection request fails to successfully copy the current usage data, then the collection file is placed in the `<InstallDir>\AUM Agent\Usage Manager\Collect` directory with the file name *DatabaseName*.USDBase, where Database Name is the file name set in the DBNAME instance of the PRIMARY.USAGE.UMDBASE class. This file can then be manually collected by copying it from the machine, or it is recreated with the latest application usage data and then collected when the agent receives the next collection request.

## Agent Processing of Data Collection Request

The monitoring process collects data for every executable that has been run on the machine. This data is saved in the active monitoring file. Since administrators need reports on what exists on the machine, but has not been used, an executable inventory is also run to augment the active usage data collected.

## Executable Inventory Scan and Options

Since the inventory capture process may take several minutes to complete, the inventory process can be configured during installation to be collected at a predefined time, daily or weekly at, for example, 1:00 A.M. Sunday. The request for data collection can aggregate the collected inventory data with the current usage monitoring data at the time of the collection request. Also, the inventory collection can be configured to run at the time the collection request is issued to provide a more up-to-date inventory. Since the executable file inventory scan can take several minutes, the request for collection is performed synchronously once the inventory scan has finished.

## Initiating Collection of Agent Data

Collection of monitoring data is initiated by running an executable with the appropriate command line parameters. Each collection request is SQL database-specific and the technique of launching an executable enables one or more collection requests to the same agent computer for either the same or differently filtered data destined for different SQL databases.

**Note:** The usage time for appropriate applications is collected based on parameters that you



select. This usage time should not be confused with focus time (the time that an application was in focus, that is, the active window in the forefront on a user's desktop).

## Portal Web Services and the Application Usage Manager

The Application Usage Manager requires components that run under the control of a Portal or another RCA server's Web Services. The Portal or Integration Server provide Web services that are shared by all loaded modules in their respective resource control file (`http*.rc`), resulting in a single entry point for all HTTP (Web-based) requests. The Application Usage Manager leverages the abilities of these servers to perform HTTP-based file copying. If the Portal or Integration Server is secured using SSL, HTTPS-based file copying is supported.

The Portal can be used to move the application usage data collection files from the monitored machines to one or more server directories. From the server directories, the data are imported into a database.

## Chapter 2

---

# Configuring Your Environment

This chapter provides information on configuring your environment to improve the database performance. This chapter also describes how to configure RCA Knowledge Base Server.

## Database Performance and Maintenance

An `Optional_Features` folder within the `<InstallDir>\Media\usage` folders include scripts and views that can be applied to a database to enhance the database performance.

**Note:** The script names may abbreviate Materialized to Mat, as in: `StepX_Define Filter Mat Tables and Indexes.sql`.

## Using Standard Materialized Views and Filtered Materialized Views

The Materialized Views are used to enhance reporting view. Either one can be optionally applied to a database to improve its performance.

- **Standard Materialized Views (SMV)**  
A feature where all the views are converted into tables and indexes are added to enhance the query speed.
- **Filtered Materialized Views (FMV)**  
A feature similar to SMV, but differs in that it requires filters to be applied at the time the views are converted into tables. The filters are stored in a separate table. As an example, if a filter for `Notepad.exe` is selected, the FMV table is populated with only notepad details for all the devices. In this way, the customer can choose to see only those applications which are important to them.

## Applying the Scripts for SMV or FMV:

1. Stop the service for the RCA Knowledge Base Server. The service can be stopped and started through the Administrative Tools options of Windows Control Panel.
2. Use normal procedures to execute the database scripts, in the given order, provided in the following locations:
  - For SQL Server:  
`<InstallDir>\Media\usage\Optional_Features\SQL Server\Filter Materialized Views`  
  
Or  
  
`<InstallDir>\Media\usage\Optional_Features\SQL Server\Std Materialized Views`

- For Oracle:  
`<InstallDir>\Media\usage\Optional_Features\Oracle\Filter Materialized Views`  
  
Or  
  
`<InstallDir>\Media\usage\Optional_Features\Oracle\Std Materialized Views`

Each of the above locations also includes a script to remove the view from your database. For example, for SQL Server and Filtered Materialized Views, the script name is:

`SQLServer-Remove Filter Mat Tables and Indexes.sql`.

## Optional Utility Scripts

As a database administrator, use the following scripts to enhance the reporting view performance:

- `Purge_Computer_Data`: Deletes all data associated with the computer name. The computer name should be provided at the appropriate place in the script. The default value is MYCOMPUTER.
- `Purge_User_Data`: Deletes all data associated with the computer name and the user name. The computer name and the user name should be provided at the appropriate place in the script. The default values are MYCOMPUTER and BOB.
- `Delete All Windows OS Files from Database`: Deletes all Windows Operating System (OS)-related files from the Usage database.
- `sp_PurgeNonCurrentComputers`: Deletes all the data associated with the device, which is not active based on the parameters passed to it and the last collection date of each device.

For example, `sp_PurgeNonCurrentComputers(90)` procedure deletes all non-current devices and data associated with it, if the last collection date is more than 90 days of time.

## Miscellaneous Scripts for Oracle

Miscellaneous scripts are additional scripts that can be applied along with the utility scripts to enhance the reporting view performance.

- `Optional_Create_Public_Synonyms`: Creates public synonyms. The script may have to be edited for the Usage Manager's user names.
- `Optional_Drop_Public_Synonyms`: Drops the public synonyms created by using the `Optional_Create_Public_Synonyms` script.
- `Step99a_DropAll.sql`: Drops all the tables present in the Application Usage Manager database.

## Concept of Current Computer

The term Current Computer refers to the device that is currently in use or is active in the network. A Non-Current Computer refers to a device which no longer exists in the network for various reasons, such as, the device has been removed from the network or it has been renamed.

The Application Usage Manager database contains information on all current and non-current devices and makes it available for reporting whenever required. By default, the Reporting Server provides reports containing information on all the devices. However, you can customize the content of the reports by categorizing the devices as Current Computers and Non-Current Computers.

The following command enables you to categorize the current and non-current devices in the database:

For Microsoft SQL Server and Oracle,

```
UPDATE rcaWindowsComputerUsers set CurrentComputer= 1 where  
ComputerName = 'MYComputerName'
```

The above command sets the **CurrentComputer** value to 1 for the device **MyComputerName** in the **rcaWindowsComputerUsers** table and signifies that the device is a current device. The value 0 in the **CurrentComputer** signifies that the device is a non-current device.

**Note:** The default value in the **CurrentComputer** column is 1. Therefore, all the devices in the network are considered current devices.

Instead of manually changing the **CurrentComputer** values in the table using the **UPDATE** command, you can use the **sp\_FlagCurrentComputers** stored procedure to flag the device to 0 or 1, that is, current or non-current device based on the parameter passed to it.

For example, **sp\_FlagCurrentComputers (90, 30)** procedure checks the last collection date of all the devices and marks the devices as current if the last collection date is within 30 days of time. If the last collection date is more than 90 days, it marks the device as non-current or not active device. The devices falling in between these two conditions remain unchanged.

**Note:** The **sp\_FlagCurrentComputers ()** procedure only flags the device to 0 or 1. It does not delete or purge the data associated with the device.

For more information on how to purge the data, see ["Optional Utility Scripts "](#) on previous page.

## Configuring the RCA Knowledge Base Server

The configuration of the KB Server is controlled through the KB Server Configuration control panel.

Complete the following tasks to configure the KB Server:

### Task 1: Access the RCA KB Server Configuration from Control Panel

1. Click **Start > Control Panel**.
2. Double-click the **RCA KB Server Configuration** icon.

The Radia Client Automation Knowledge Base Server Configuration window opens.

### Task 2: Configure the KB Server automated import directories

1. Click **Add** in the Radia Client Automation Knowledge Base Server Configuration window, to add a new Knowledge Base data source. The New Knowledge Base – Configuration dialog box opens.

2. Enter the following information:

Knowledge Base Name:	Type the Knowledge Base name (Any name of your choice).
Data Source Name:	Type the Data Source Name (DSN).
User Name:	Type a user ID that has owner authority for the database.
Password:	Type a valid password for the user ID.

**Note:** The KB Server administrator must supply a login ID and password for the person who has rights to access the SQL database. This ID must have full access rights to the database objects including table and stored procedures. Type the ID with these rights and its password.

3. Click **OK**.

### Task 3: Edit the Global Settings

To complete the Knowledge Base configuration, edit the Global Settings, located at the bottom of the Radia Client Automation Knowledge Base Server Configuration window:

- **Log Path**  
Default log path for AutoImport processing status information. All exceptions are logged. Successful imports and file deletions after successful imports of Client Automation Service state files are also logged.
- **Log Level (default is Errors/Other)**  
The log level determines how much data is logged to the KB Server log file. There are three possible settings:
  - **Errors Only** – Records only errors.
  - **Errors/Other** – (Recommended) Records errors and other important information. In large environments, recording more than errors to the log file can result in very large file sizes.
  - **Verbose** – Defines additional information on successful processing into the database.
  - **Debug** – Records detailed information about KB Server activities, including successful activities. Debug log level should only be used at the request of Persistent Support.
- **Database Reconnect (msecs)** (default is 5000)  
Number of milliseconds to wait between reconnect attempts to the database server.
- **Import Directory Scan (msecs)** (default is 5000)  
Number of milliseconds to wait between each check of the import directory for new files.
- **Switch Tasks after (mins)** (default is 1)  
Number of minutes to wait before switching to the next scheduled task.

A new Knowledge Base is now available. After you finish adding a Knowledge Base, you can add Tasks that run against your databases.

### Task 4: Creating Tasks

You can create Tasks associated with each Knowledge Base to populate and modify your RCA Configuration Server Database (CSDB).

1. Click **Add Task** on the RCA Knowledge Base Server Configuration window.
2. Click the **Task Type** arrow.
3. From the **Task Type** list, select one of the following:
  - **RCA Application Usage Manager Collection Files**  
Create a task of this type to define your automated import directory for usage files that are collected.
  - **RCA Configuration Server DB Product-to-Application Rule Extracts**  
Use this task to import rules which are extracted from the RCA Configuration Server. These rules are imported into the Application Usage Manager Database. Imported rules are viewed and modified using the Application Usage Manager Administrator and are used in the Server Web Reports for filtering the usage data.
    - **RCA Application Usage Manager Purge Criteria**  
  
Use this task to purge usage data from your database. You must define whether the purging will take place daily, monthly, or yearly.  
  
Recommended settings:  
  
Daily: 31-62 days  
  
Monthly: -1  
  
Yearly: -1
  - **RCA Application Usage Manager Move File(s)**  
Use this task for usage file collection failover support, to move the USDBase files from your Error directory, your Archive directory, or both, to the import directory for usage collection. Specify the Import Directory on the RCA KB Server - Add Task window. This task occurs at midnight.
4. The type of task you select will determine what information is required in the following text boxes. Depending on the task you select, some of these text boxes may not appear.
  - **Task Name**  
Type a name for the task, for example, Collection Files.
  - **Import Directory**  
Enter the path for the directory from which files will be imported. Use Browse to navigate to it.
  - **After Import**  
Select the action to be taken after import: **Archive** or **Delete**. This option allows you to remove the files from the import directory immediately after they are imported.
  - **Retry Errors**  
For the RCA Application Usage Manager Move File(s) task, select the **Retry Errors** check box to move all the files from the Error directory to the import directory. From the import directory, the KB Server automatically imports them into the database. Use Retry Errors after a previous collection error due to a network or database communications error.
  - **Retry Archives**  
For the RCA Application Usage Manager Move File(s) task, select the **Retry Archives** check box to move all the files from the Archive directory to the import directory. From the

import directory, the KB Server automatically imports them into the database. Use Retry Archives only when your database is corrupted or new.

5. Click **OK** and you are returned to the RCA Knowledge Base Server Configuration window. It now displays the Task Name and Directory information you just entered.
6. Click **Save Configurations** to save all the configuration changes.
7. Restart the KB Server.

## Starting and Stopping the KB Server

The KB Server is controlled as a Windows service. The friendly service name is **RCA Knowledge Base Server** and the executable is `hpkbmanager.exe`. The service may be stopped and started through the Administrative Tools options of the Control Panel.

## SQL Server Requirements for the KB Server

To process Knowledge Base requests, the KB Server requires a SQL Server or Oracle logon ID. A user ID of any name can be configured (the default is **sa** for SQL Server or **usage** for Oracle). This ID is used to define the DB\_OWNER for the Knowledge Base database with full permissions for administering the database. This ID is referred to as the AppLogin user ID.

## Chapter 3

---

# Aggregation of Usage Data Files with Tier-Level Store and Forward

This chapter describes the aggregation process and how to configure store and forward to improve the performance in your environment.

## Introduction

The Aggregation of Application Usage Manager data files (USDBase files) with Tier-Level Store and Forward support is based on the methodology that the USDBase files pass through a set of existing upstream servers within a centralized network (Store and Forward Messaging Servers), which reduces the need to install multiple Usage Databases and KB Servers. The Store and Forward Messaging Servers accept the incoming USDBase files and forward them to another upstream server. Upon receipt and prior to being forwarded, the USDBase files undergo an Aggregation process.

Making use of tiered store and forward servers with aggregation tools drastically improves scalability and reduces large-scale issues that can arise when dealing with large numbers of Application Usage Manager agents (Usage agents) across an enterprise. When using store and forward aggregation, a single KB Server can support much larger numbers of Usage agents, as well as show improved performance when supporting the same number of Usage agents.

## Aggregation

Aggregation is a process of merging two or more USDBase files into a single USDBase by eliminating all the duplicate data among the USDBase files.

When the KB Server imports the usage data, it must query the database for each import data record to check for its existence, and then updates the database accordingly. If there are N number of files with common data to import, the KB Server has to query the database N number of times. If the data in these common files can be aggregated into a single file, the KB Server only needs to query the database and update it once. Thus, aggregating the data for common files prior to import improves the KB Server performance enormously.

An aggregated file contains only a single reference of a data for each file involved in aggregation. This reduces the size of an aggregated file and the overhead of multiple queries to the database when importing.

## Implementation

The Messaging Server's Store and Forward capability is used to implement the Usage Data Files Store and Forward. The Messaging Server is responsible of storing all the USDBase files, trigger the aggregation process once the trigger constraint is satisfied, and forward the aggregated file.



In the non-Store and Forward scenario, all the Usage agents send their USDBase collection files to a predefined collection point that is monitored by KB Server which in turn extracts the usage data from the files collected from each agent computer and loads this data into your SQL-enabled database, making the data available for reporting purposes.

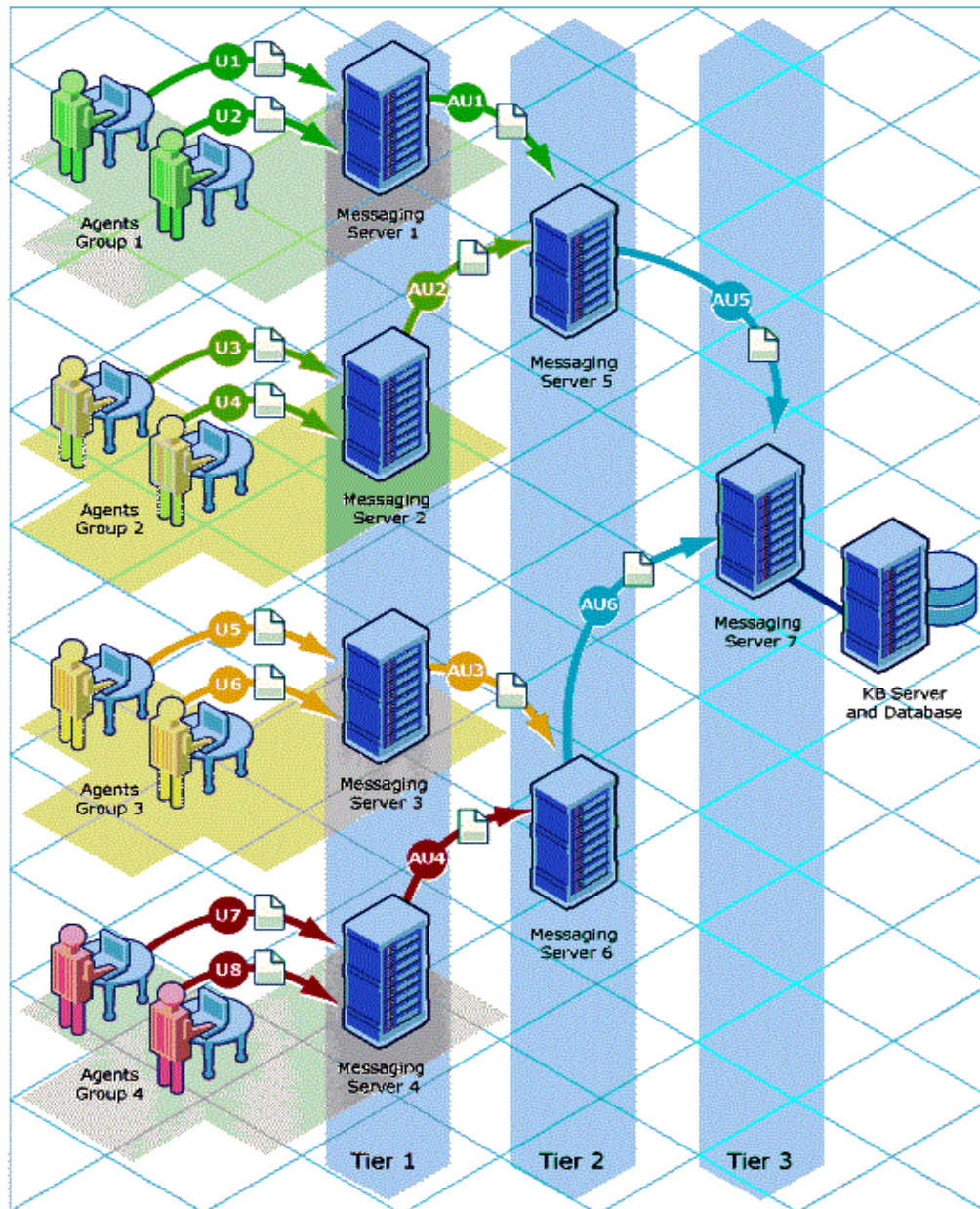
With Store and Forward, all the Usage agents send their USDBase collection files to a Messaging Server. We can have multiple such Messaging Servers in an enterprise to form a tier level architecture. The tier-level architecture should be implemented according to the number of Usage agents available in that Enterprise to get better performance.

In an n-tier level architecture, the level 0 is the tier with only the Usage agents, level n is the final tier having the Portal installed with KB Server configured for importing USDBase files. All middle level tiers have Messaging Server with Aggregation enabled and may have Usage agents. Each middle level can have one or more Messaging Servers configured to forward the aggregated USDBase file to the next level Messaging Server.

All the Usage agents must be configured to send their USDBase collection files to its immediate next level tier Messaging Server. This is the only change required in the Usage agent needed to implement Store and Forward Aggregation.

Once the Messaging Server in a middle tier receives the USDBase files, depending on the configurations set it triggers the Aggregation Process by executing the `USDBAggr.exe` which is the tool for performing Aggregation. After the Aggregation Tool is successfully executed, the Messaging Server transfers the aggregated USDBase file to the next tier server. If the next tier is one of the middle level tiers, then the aggregation process continues till it reaches the final tier. If the next tier is the final tier, then the aggregated USDBase file gets imported into the database by the KB Server.

The following figure illustrates a multi-tiered Messaging Server architecture used to provide aggregated USDBase files for import into the usage database.

**Tier-Level Architecture for Usage File Aggregation**

## Configuring Usage Data Files Store and Forward

You can configure your environment to store and forward usage data files to enhance the performance.

This section describes various sections and parameters in the `usage.dda.cfg` file and how to configure aggregation in your environment.

## Configuring Aggregation

1. Configure the entries in the `usage.dda.cfg` file, as explained in the section "[About the Sections in the USAGE.DDA.CFG File](#)" below.
2. Following configuration, restart the **RCA Messaging Server** service.  
You can have multiple tiers of Messaging Servers performing aggregation. The URL parameter in the **msg::register usage-forward** section of the `usage.dda.cfg` determines whether the aggregated usage data is forwarded to the next-tier Messaging Server, or to a KB Server import location.

## About the Sections in the USAGE.DDA.CFG File

The `usage.dda.cfg` file in the Messaging Server defines the configurations available for Aggregation. The file has the following main sections after the header and the required lines.

```
# DO NOT REMOVE FOLLOWING LINE
```

```
package require nvd.httpd
```

### **msg::register usagehttpd**

This is the HTTPD Section Type for the `usage.dda` configuration. If the Messaging Server is receiving USDBase files from one or more Usage agents or another Messaging Server, define the URLHANDLER location on which to look for the files. This location is the source folder for the Aggregation Tool.

The parameters in the URLHANDLER are summarized below:

**USE** defines the name of AGGREGATE Type that receives the incoming file.

**DIR** defines the directory for the HTTPD Type.

**URL** defines the prefix that that is accepted by the Messaging Server. When messages are received with the designated URL they are deposited in the associated queue.

**HTTPMETH** defines the method used by the Usage agent to transfer the file. Set the HTTPMETH type to PUT.

### **msg::register usage-aggregate-queue-in**

This is the AGGREGATE Type section for the `usage.dda` configuration. This defines the Aggregation Queue in which the USDBase files are queued up for processing by the aggregation tool.

**DIR** defines the source directory for the Aggregation Tool. This should be same as that of the HTTPD Type.

**USE** defines the name of the HTTP Type that forwards the aggregated file.

**COUNT** defines the minimum number of USDBase files expected in the DIR directory to initiate the Aggregation Process. The default is **400**. The Administrator can configure the COUNT.

**POLL** defines the interval, in seconds, used to poll the source DIR directory for USDBase files.

**TIMEOUT** defines the maximum interval to wait, in minutes, for the number of USDBase files to reach the COUNT.

**USER\_DEFINED** is a flag to enable a user-defined procedure to execute whose return value controls the triggering of the Aggregation. Set to `Y` if a user-defined procedure is to be used. When set to `Y`, the COUNT and TIMEOUT parameter are ignored, and the UD\_TCL\_FILE and UD\_PROC parameters must be used to define the location and procedure name to execute.

**UD\_TCL\_FILE** defines the fully-qualified path to the TCL file containing the user-defined procedure, when USER\_DEFINED is set to `Y`.

**UD\_PROC** defines the user-defined procedure name to execute, when USER-DEFINED is set to `Y`.

**USDBAGGRPATH** defines the full path of the Aggregation Tool.

**TARGET** defines the fully-qualified path to the directory where the aggregated USDBase file is placed.

**ERRORPATH** defines the fully-qualified path to the directory where the erroneous USDBase file is moved from the DIR directory.

**ARCHIVE** Set to `Y` to archive the USDBase file after aggregation; set to `N` to delete the USDBase file after aggregation.

**ARCHIVEPATH** defines the fully-qualified path of the directory where the USDBase file is placed when ARCHIVE is set to `Y`.

**MAXSIZE** defines the maximum size, in bytes, for the generated aggregated file.

**Note:** If the Input USDBase file size is larger than the MAXSIZE, the file is not aggregated and is sent without any modification.

**LOGPATH** defines the fully-qualified path of the directory where the log files are written by the aggregation tool.

#### **msg::register usage-forward**

This is the HTTP Type for the `usage.dda` configuration. This defines the forwarding server to which the aggregated file is sent.

**PRI** denotes the priority in which to send the files to the companion URL. The default Priority is **10**. This setting only matters if multiple ADDRESS entries are configured.

**URL** specifies the URL to use to send the aggregated file. This URL entry uses the same syntax as the COLLDST for the Usage agents, discussed on ["Configuring the Application Usage Manager Agent for Distribution" on page 32](#).

- To send the aggregated USDBase file to a Portal that has the KB Server installed on it, code the URL as:  
URL `http://Portal_IP:3471/KB_Mgr1_Usage/`
- To forward the aggregated USDBase file to the next tier Messaging Server enabled for the aggregation of usage data, code the URL as:  
URL `http://messaging_svr_IP:3461/proc/usage`

**Note:** If the target servers are SSL-secured, adjust the URL syntax to include https and the secure port number.

For more information on these section types, see the *Radia Client Automation Enterprise Messaging Server Reference Guide*.

## Performance

You must fine-tune the configuration parameters in **usage.dda.cfg** to obtain the best aggregation performance. The main parameters that need tuning include:

**MAXSIZE** – This parameter directly impacts the compression ratio of an aggregated file, because MAXSIZE determines the number of files that can be placed in an aggregated file.

**COUNT** – This affects the MAXSIZE. Make sure the number of files in COUNT is sufficient enough to reach the aggregated file size set in MAXSIZE.

**POLL** – This parameter determines how often the files are collected from the source folder.

# Chapter 4

---

## Application Usage Manager Agent

This chapter describes how to configure Application Usage Manager Agent for distribution. This chapter also describes various filters to be used to collect usage data, how to apply these filters, and how to initiate inventory and usage collection.

### The USAGE Domain Defined

The Application Usage Manager utilizes the USAGE Domain within your Configuration Server Database, enabling management of the Application Usage Manager in the enterprise. The USAGE Domain is comprised of classes that you use to create Application Usage Manager services to distribute to your agent computers. These services install the Usage agent, which collects Application Usage data based on your specifications. The next few sections describe the USAGE Domain classes.

Use the CSDB Editor to configure each class in the USAGE Domain.

#### USAGE Domain Classes

Class	Description
Application (ZSERVICE)	Contains the Application Usage Manager services.
Application Packages (PACKAGE)	Contains the Application Usage Manager packages.
Client Methods (CMETHOD)	Client methods used to process each instance.
Collection (UMCOLLECT)	Controls the Application Usage Manager collection options that represent the unique collection criteria with which the USDBase collection files on each computer are associated. A single computer may have multiple collections targeted, each associated with a unique data store. The collection file contents are sent to different collection points and ultimately to different SQL databases.
Configuration (UMCONFIG)	Controls the Application Usage Manager installation options.
Database (UMDBASE)	Unique usage database name, which correlates to a backend SQL database.
Destination Point (UMDESTPT)	Location where Application Usage data is stored.

Class	Description
File Resources (FILE)	File instances included within a package.
File Root (FILEROOT)	Defines the base location of a file without any extended path information. The path can be a drive, like C: \, or a well known folder location, like ProgramFiles folder.  File Roots are only used for filtering the collection file content collected from the agent in the CSDB Editor.
Filter Criteria (UMFLTCRI)	Defines usage filtering criteria.
Filter Rule (UMFLTRUL)	Connects to usage filtering criteria. The filter type determines whether it is an inclusion or exclusion Filter Rule, and its priority determines its importance when compared with other Filter Rules defined in a Filter Set. For more information, see <a href="#">"Filters" on page 36</a> .
Filter Set (UMFLTSET)	Connects to one or more Filter Rules. Filter Sets are in turn connected to collections in the UMCOLLCT Class. Each UMCOLLCT Class may then have specific filtering associated with its data collection.
Inventory (UMINVENT)	Defines default configuration criteria for the Application Usage Manager inventory scan.
Path (PATH)	A unique path to one or more components.

## Significance of Collection Instances

Collection class instances, and their related filter class instances, establish the content that is uploaded to a specific SQL database from the device which the Application Usage data is collected. Collection class instances define the database-specific agent collection properties; they also define the destination location once the usage and inventory data has been aggregated on the agent machine and is ready to be passed through the network for import into a specific SQL database.

## Configuring the Application Usage Manager Agent

The Application Usage Manager agent is installed as a service to the existing RCA Agents in your environment.

The Application (ZSERVICE) class in the USAGE Domain contains **Application Usage Mgr Agent – Core** service that requires minimal configuration. Connect **Application Usage Mgr Agent – Core** service to the appropriate agent machines to distribute the Application Usage Manager agent. The Application Usage Manager agent is distributed during the next agent connect.



Use the **Application Usage Mgr Agent – Core** service to define inventory and collection parameters, and for distribution to your agent computers.

## Viewing Attribute Description and Name in the Application Class Instance Attributes

1. Start the RCA Administrator CSDB Editor and double-click to expand the PRIMARY.USAGE class.
2. Double-click to expand the **Application (ZSERVICE)** class.
3. From the Menu bar, go to **View >Options**. The Options window opens.
4. Select the **Instance Options** tab.
5. Under **When Displaying Instance Attributes, Show Attribute**, select the **Both** button.
6. Click **OK**.
7. Close the CSDB Editor and log on again.

## Configuring the Application Usage Manager Agent for Distribution

1. Start the RCA Administrator CSDB Editor and double-click to expand the PRIMARY.USAGE class.
2. Double-click to expand the **Application (ZSERVICE)** class.  
This class contains several services you can use to distribute the Application Usage Manager agent as well as apply any collection filters. The service **Application Usage Mgr Agent – Core** distributes the Application Usage Manager agent to your environment and contains a default collection instance.
3. Double-click to expand the **Application Usage Mgr Agent – Core** service.  
The service contains four configurable connections:

Application Usage Manager Agent	Application (PACKAGE) instance
Configuration – CCM	Configuration (UMCONFIG) instance
Inventory – First of the Month	Inventory (UMINVENT) instance
Collection – CCM	Collection (UMCOLLECT) instance

4. Right-click **Configuration – CCM**.
5. In the shortcut menu, select **Edit Instance**. The Editing Configuration-CCM Instance dialog box opens.
6. To edit the instance, select **SERIAL** from the attribute list. Enter your Application Usage Manager serial number.
7. Click **OK** to close the window.
8. Double-click to expand **Collection – CCM**.



9. Double-click to expand **HTTP - CMIS\_IP\_ADDR:Port\URL**.
10. Double-click **COLLDEST** from the attribute list and enter the URL and port of the RCA Server used to collect the USDBase files from the RCA Agents in your environment.
  - If you are using Messaging Servers enabled for usage aggregation to collect USDBase files from the RCA Agents, specify COLLDEST using the hostname and the listening (store and forward) port of your Messaging Server as follows:  
**http://1.1.1.10:3466/proc/usage**  
 or  
**https://1.1.1.10:3466/proc/usage**
  - If you are using a Portal to collect USDBase files from the RCA Agents, use the following example:  
**http://1.1.1.10:3471/KB\_Mgr1\_Usage/**  
 or  
 If your Portal has been SSL-secured, specify the **COLLDEST** url using **https**, such as:  
**https://1.1.1.10:443/KB\_Mgr1\_Usage/**
  - By default, the Core uses Apache Server to collect the USDBase files from the RCA agents using the following example:  
**http://1.1.1.10:3466/KB\_Mgr1\_Usage/**  
 or  
 If your Apache Server has been SSL-secured, specify the **COLLDEST** URL using **HTTPS**, such as:  
**https://1.1.1.10:3466/KB\_Mgr1\_Usage/**

The KB Server monitors this collection point and moves any files it finds into your SQL database for viewing. After the files are moved out of the collection point, they are saved in a subdirectory called *Archive*.

The default collection parameters are described in the following table.

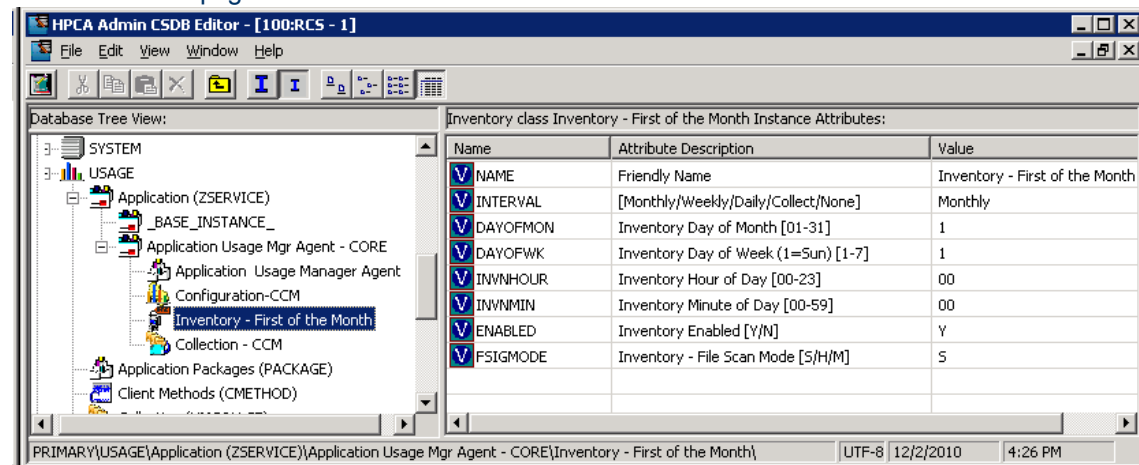
#### Default Collection Parameters (UMCOLLECT)

Instance	Default Value	Description
NAME	Primary Collection Parameters	Friendly Name.
INTERVAL	Weekly	When the collection will take place. [Monthly/Weekly/Daily/None]
DAYOFMON	1	Day of the month collection will take place. [01-31]
DAYOFWK	1	Day of the week collection will take place. [1=Sun] [1-7]
COLLHOUR	00	The hour of the collection. Midnight is hour 00.

Instance	Default Value	Description
		[00-23]
COLLMIN	00	The minute of the collection. [00-59]
COLLRAND	0	Randomized Collection. Maximum delay minutes to use to randomize the collection start time. If non-zero, randomizes the collection process to occur anytime from the start time through a randomly generated number of minutes later. [0-720]
ENABLED	Y	Whether or not collection is enabled.
COLLCNCT		Collect on RCA Agent Connect? [Y/N]  <b>Note:</b> CA Agent Connect now refers to an RCA Agent connect.
DBASCONN	USAGE.UMDBASE.PRIMARY	Usage database connection.
DESTCONN		This is a connection to a predefined collection point. This is the location where files are stored until the KB Server moves them into your SQL database.
CMETHOD	CMETHOD.UMCOLLCT	The collection method.
FLTSET01	USAGE.UMFLTSET. USAGE_INCLUDE_ ALL_FILES	Filter Set connection.
FLTSET02 through FLTSET10		Filter Set connections.

11. Double-click the attribute **IPVER** and specify the IP version through which the communication should happen. For more information on configuring the attribute IPVER, see the *Radia Client Automation Enterprise User Guide*.
12. Click **OK** to close the dialog box.
13. Connect any Filter Sets you would like to include with your service by dragging the Filter Set instance onto the service name. For more information on how to create and apply filters, see

"Filters" on next page.



If you want to adjust the inventory time, double-click **Inventory – First of the Month**. The following table describes each inventory parameter.

#### Default Inventory Parameters (UMINVENT)

Attribute	Default Value	Description
NAME	Default Inventory Parameters	Friendly Name
INTERVAL	Weekly	When each inventory takes place. [Monthly/ Weekly/ Daily/Collect/None]
DAYOFMON	1	The day of the month to begin the inventory. [0-31]
DAYOFWK	1	Day of the week each inventory takes place. [1-7] (1=Sunday)
INVNHOUR	00	The hour of the day at which the inventory takes place. [00-23]
INVNMIN	00	The minute at which the inventory takes place. [00-59]
ENABLED	Y	Whether or not inventory is enabled.
FSIGMODE	S	<p>Three levels of scanning depth for executables inventoried on each agent device are available. The type of scan defined here can determine the amount of time a collection may take.</p> <p><b>S</b> File Sizes Only. Faster, less comprehensive (default)</p> <p><b>H</b> Entire Module Header. Slower, more comprehensive</p> <p><b>M</b> Complete MD5 Signature. Slowest, most</p>

Attribute	Default Value	Description
		comprehensive
CMETHOD	CMETHOD.UMINVENT	The inventory method.

These parameters can be adjusted to adhere to your specific requirements. The default inventory begins on the first of the month and repeats once a week every Sunday at midnight.

## Filters

By default, the Application Usage Manager collects usage information for every executable installed on the agent computer. To collect only specific executable information, filters can be defined and attached to the collection instance. Because all executable information is collected by default, the **Exclude All** filter rule must be included with any filters you use.

The USAGE Domain contains classes associated with creating filters for your usage data. This enables you to collect specific information based on parameters you define. The filter related classes are:

- Filter Criteria
- Filter Rule
- Filter Set

Each of these classes contains configurable instances you can use to define your filter.

RCA also contains pre-configured Collection Filters by default. You can use these filters as models for creating new filters, or you can modify these filters to suit your needs. For more information, see Chapter 8, *Operations* in *Radia Client Automation Enterprise User Guide*.

## Criteria, Rule, and Set

To help you define filter parameters, the Application Usage Manager uses filter criteria, rules, and sets.

- **Criteria**  
Criteria are specific attributes that an application can contain, for example, member of the Microsoft family of applications.
- **Rule**  
When multiple criteria are combined, they form a rule. A rule is a simple way of grouping criteria, making it easier to apply the same set of criteria to multiple services.
- **Set**  
When multiple rules are grouped into one instance, a set is created. A set is the highest level of criteria collection containing multiple rules, which in turn may contain multiple criteria.

## Filter Criteria Class (UMFLTCRI)

The Filter Criteria Class contains various instances that reflect vendor-specific applications. Use these to attach a filter criterion using one of the included applications. The instances include filter criteria for Compaq, McAfee, Microsoft, and InstallShield, as well as many others.

## Filter Rule Class (UMFLTRUL)

The Filter Rule Class contains pre-configured rules using common vendor-specific parameters. For example, Include Microsoft Office Products includes all Microsoft Office applications, and Exclude Microsoft Windows excludes all Microsoft Windows files.

This Filter Rule Class connects to the usage filtering criteria. The filter type determines whether it is an inclusion or exclusion Filter Rule and its priority determines its importance when compared with other Filter Rules in a Filter Set (Zero is the lowest priority). If the event priorities are equal within a Filter Set, inclusion filters take precedence over exclusion filters.

If no criteria are specified for an inclusion filter, then all usage information is captured in the collection file. If no criteria are specified for an exclusion filter, then all usage is excluded.

## Filter Set Class (UMFLTSET)

A Filter Set is comprised of one, or a collection of, Filter Rules. The Filter Set class contains pre-configured Filter Sets you can use to collect or exclude vendor-specific information.

After a Filter Set has been created, or you decide which existing Filter Set to use, connect it to a Collection class (UMCOLLECT) instance to enable the filter. Only Filter Sets may be connected to a collection class. All criteria associated with that Filter Set are then processed. By connecting the Filter Set to a Collection class instance, each data collection can then contain specific filtering.

### Default filter set parameters

Attribute	Default Value	Description
NAME	Default Filter Set Parameters	Filter Set Friendly Name
INCLUSAG	Yes	Determines whether or not to include usage data as well as inventory data in the collection.
CONCURR	No	Defines whether to collect concurrent usage data. For more information, see <a href="#">"Using Concurrency" on page 41</a> .
CMETHOD	CMETHOD.UMFLTSET	Client method used to process Filter Set class instances
FLTRUL##		Filter Rules connections

## Using Filters

Filters can be applied to Collection class instances. Use the existing Filter Set instances, or create your own using the filter classes provided. The following exercises explain how to apply a filter as well as how to create a new filter based on parameters you define.

## Filter Set Class Instances

The Filter Set Class (UMFLTSET) contains a few default Filter Sets that can be used for generic data collections. Each class instance collects a specific type or set of data. Following table describes each class instance in detail.

### Filter set class (UMFLTSET) instances

Instance Name	Description
All Apps – Except Base OS Apps	Collects data for all installed applications with the exception of base operating system applications.
CCM Filter Set	Collects data for the Microsoft and Internet Explorer applications defined in the Filter Criteria connections.
Concurrency – Novadigm Apps Only	Collects concurrency data.  This default setting collects data for all RCA applications. RCA applications were formerly known as Novadigm and Radia applications, as well as RCA applications.
Default Filter Set Parameters	Contains the default Filter Set instance values and is used to create custom Filter Sets.
Inventory Only – Incl All Files	Collects inventory data for installed applications - no usage data is collected.
Microsoft Licensed Applications	Collects data for Microsoft applications as defined in each Filter Criteria connection.
Usage – Include All Files	Collects all usage data.

## Applying Filters

Filters can be applied to Collection class instances by simply dragging the Filter Set instance onto the appropriate Collection class instance.

## Applying a Filter to a Collection Class

1. Start the RCA Administrator CSDB Editor and double-click to expand the PRIMARY.USAGE class.
2. Connect the appropriate Filter Set to the connection class you would like to apply the filter to.
3. Click **Copy** and accept the changes.

## Creating Filters

Filters can be created by following three basic steps:

1. Create or select a Filter Criteria instance.
2. Create or select a Filter Rule instance and attach the Filter Criteria instance.
3. Create or select a Filter Set instance and attach the Filter Rule instance.

The following example demonstrates how to create a filter collects usage information for Adobe Acrobat.

### Creating a Filter Criteria Instance

1. Start the RCA Administrator CSDB Editor and double-click to expand the PRIMARY.USAGE class.
2. Double-click to expand **Filter Criteria (UMFLTCRI)**.
3. To create a new instance, right-click **Default Filter Criteria Params** and select **Copy Instance**, from the shortcut menu. The Copy Instance dialog box opens.
4. Rename the new instance **Adobe Acrobat**, and then click **OK**.
5. In the tree view of the CSDB Editor, double-click the newly created instance. The Editing Instance dialog box opens.

Use the attributes defined in the following table to define your filter criteria.

#### Filter Criteria Attributes

Attribute	Description
NAME	Friendly Name
ROOTCONN	Compares for applications that reside in any of the predefined shell folder names, such as ProgramFilesFolder, WindowsFolder, or SystemsFolder. These can be used to filter based on a well-known folder, such as TempFolder.
DESCRIPT	Description of filter criteria.
ENABLED	Whether this filter is enabled or not. [Y/N] Default is <i>Y</i> .

Attribute	Description
FILEROOT	Defines the file root path, or the base location of a file without any extended path information. Can be a drive, like C:\, or a well known folder location, like ProgramFiles folder.
FILEPATH	Defines the suffix of the path name that is appended to the file root path. For example, this would contain the characters \Microsoft Office regardless if the installation for the Microsoft Office application was to the ProgramFilesFolder\Microsoft Office path or to the TempFilesFolder\Microsoft Office path.
FILENAME	The application file name executable, for example winword.exe.
COMPNAME	The vendor name defined in the executable's header.
PRODNAME	The product name defined in the executable's header.
PRODVER	The product version defined in the executable's header.
FILEDESC	The file description defined in the executable's header.
FILEVER	The internal file version defined in the executable's header.
ORIGNAME	The original file name defined in the executable's header. This string does not change if the file is renamed.
MD5HASH	The MD5 hash file signature that uniquely identifies the contents of the file. Any change to a file assigns a unique MD5 hash signature to the file.
CMETHOD	The client method used to process Filter Criteria instances.

- Double-click the **COMPNAME** attribute from the attributes list. The Editing Instance dialog box opens.
- Type **Adobe** in the Company Name text box.
- Click the **PRODNAME** attribute and type **Acrobat**.
- Click **OK** and save the changes.

You have successfully created a new Filter Criteria instance.

## Creating the Filter Rule Instance

- Start the RCA Administrator CSDB Editor and double-click to expand PRIMARY.USAGE class.
- Double-click to expand the **Filter Rule (UMFLTRUL)** class.
- Right-click **Default Filter Rule Parameters** and select **Copy Instance**, from the shortcut menu. The Copy Instance dialog box opens.
- Rename the new Filter Rule instance **Adobe Apps**, and click **OK**.



5. In the CSDB Editor window, connect the Filter Criteria instance you created, Adobe Acrobat, to the newly created Adobe Apps Filter Rule instance.
6. Click **Copy**.
7. Click **Yes** to accept the changes.
8. Click **OK**. The Filter Criteria instance is now connected to a Filter Rule instance.
9. In the list view of the CSDB Editor, double-click the PRIORITY instance attribute and set the value to 1 to ensure this rule is applied before any default rules are used. (Zero is the lowest possible priority as well as the default value.)

The Filter Rule instance is now complete.

## Creating the Filter Set Instance

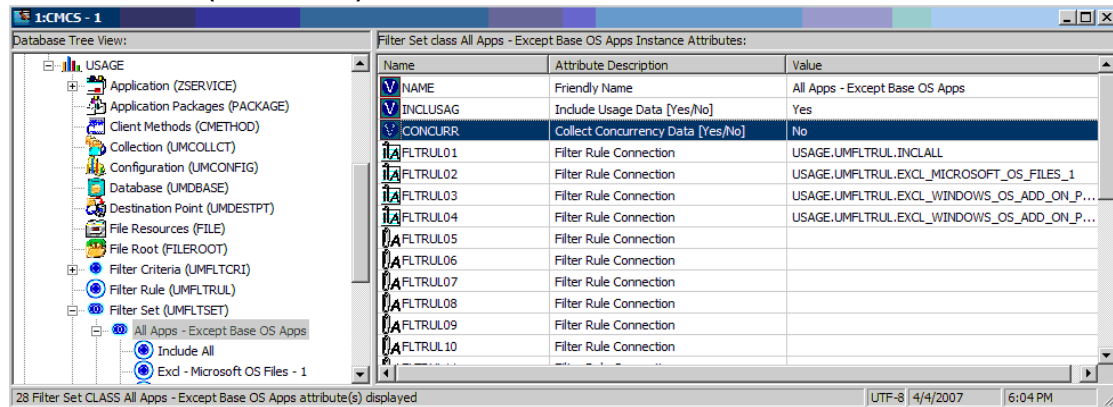
1. Start the RCA Administrator CSDB Editor and double-click to expand PRIMARY.USAGE class.
2. Double-click to expand the **Filter Set (UMFLTSET)**.
3. Right-click **Default Filter Set Parameters** and select **Copy Instance**, from the shortcut menu. The Copy Instance dialog box opens.
4. Rename the new Filter Set instance `Adobe Licensed Applications`.
5. Connect the Filter Rule instance you created earlier, Adobe Apps, to the newly created Adobe Licensed Applications Filter Set instance.
6. Also connect the existing Filter Rule instance, Exclude All, to the newly created Filter Set instance. This ensures that only usage data for the specific executable defined in your criteria, Adobe Acrobat, is collected.  
By default the priority setting for this instance is 0, the lowest possible. By setting the priority for the Adobe Apps rule to 1 earlier, you have given priority to that Filter Rule instance, ensuring it is applied before any default rules.

The Filter Set instance is complete. You are now ready to apply the filter to a collection instance. For more information, see the section "[Applying Filters](#)" on page 38.

## Using Concurrency

Data usage collection is available either on a daily basis or on a more specific basis using concurrency. Concurrent data collection is enabled at the Filter Set level (UMFLTSET) in the CONCURR instance attribute.

### Filter Set Class (UMFLTSET) CONCURR instance



## Enabling Concurrency Usage Data Collection

**Caution:** Concurrent usage data collection generates a large amount of data. Make sure you have enough available resources before you begin collecting this type of data.

1. Navigate to an existing Filter Set instance. For more information, see ["Creating the Filter Set Instance" on previous page](#).
2. Double-click the **CONCURR** instance attribute.
3. From the list, select **Yes**.
4. Click **OK**. Click **Yes** to save your changes.  
Concurrency usage data collection has been enabled. Concurrent usage data will now be collected for the appropriate applications in 15 minute intervals, by default.

## Initiating Inventory and Usage Collections

The executables, `USDBInvn.exe` and `USDBCcoll.exe` can be used to initiate the collection of inventory and usage data respectively. After a default installation, these files are located in the `\Program Files\Hewlett-Packard\HPCA\AUM Agent\bin\` folder.

### Initiating Inventory Data Collection

The executable `USDBInvn.exe`, collects current inventory data on a target machine. Run this executable to force inventory collection for any machine with the Application Usage Manager Agent installed. No parameters are required. The inventory information is stored within the `History.USDBase` file, on the local machine at the root of the `\Usage Manager\` directory.

### Configuring Usage Data Collection

The executable, `USDBCcoll.exe`, enables you to configure the Application Usage Manager data collection environment on the agent device.

## Defining a Database Collection Point

A database definition contains the information required to send the collected usage data to a specific collection point in the backend infrastructure. It has a unique name and associated parameters.

Database entries can be configured in the Configuration Server Database in the PRIMARY File USAGE Domain. Default database and associated configuration parameters are shipped with the Application Usage Manager. To manually define a database collection point, run the following command:

```
USDBColl.exe /i DatabaseName=SQL_database_name
```

The `/i` parameter indicates an **install database** operation.

## Initiating a Usage Data Collection Request

Run the `USDBColl.exe` module to initiate a data collection request. You can initiate a data collection request by the Application Usage Manager internal scheduler, by an RCA service or Notify request, or otherwise. Any filtering is applied during the collection process.

To launch a collection, run the following command for the specific database name defined in the command line:

```
USDBColl.exe DatabaseName=SQL_database_name
```

## Initiating a Usage Data Re-collection Request

After data is collected, it is not sent to the server again during a normal collection request.

**Caution:** Recollection may result in duplicate data or a corrupted SQL database if not done within strict guidelines and without the consent of Persistent Technical Support.

To initiate a re-collection of data (data already sent to the server), follow these steps:

1. Run the following command as an administrator:  

```
USDBColl.exe DatabaseName=<UniqueSQLDatabaseName>  
RecollectMode=<value> /RecollectMode
```
2. Run the following command to start the normal usage collection:  

```
USDBColl.exe DatabaseName=UniqueSQLDatabaseName
```

This command starts the collection with `RecollectMode` specified in Step 1.

### USDBColl.EXE Command Line Parameters

Parameter	Description
DatabaseName=UniqueSQLDatabaseName	Defines a unique SQL database name for collection purposes.
RecollectMode=Value	Defines the type of data to be recollected. The value can be 1, 2, or 3 as defined below.

Parameter	Description
	<p>1 – <b>Signatures</b> - all file signature data is recollected for all files that meet the collection filter. This includes the data for the FileSignatures and FileSignatureProperties tables.</p> <p>2 – <b>Files</b> - all Windows file data is recollected for all files that meet the collection filter. This includes all of the data collected in Signature mode as well as data for the WindowsFiles and WindowsFileInstances tables.</p> <p>3 – <b>Usage</b> - all Windows file usage data is recollected for all files that meet the collection filter. This includes all of the data collected in File mode as well as data for the WindowsFileUsage table.</p>

## Enabling Privacy

The Application Usage Manager enables for the obfuscation of certain data attributes in order to ensure privacy, if required. The following information can remain undisclosed:

- **User Name**  
The user name is reported as [AnyUser].
- **Computer Name**  
The computer name is reported as a random set of alphanumeric values.
- **Domain Name**  
The domain name is reported as a random set of alphanumeric values.
- **Usage Times**  
The executable file usage times and launch counts are all reported as zero values.

Four attributes in the UMCONFIG Class directly relate to this information. Set these values to **Y** to hide the related data.

### Obfuscation attributes of the UMCONFIG class

Attribute	Description
OBFSUSER	Set this value to <b>Y</b> to obfuscate user name data.
OBFSCOMP	Set this value to <b>Y</b> to obfuscate computer name data.
OBFSDOMN	Set this value to <b>Y</b> to obfuscate domain name data.
OBFSUSAG	Set this value to <b>Y</b> to obfuscate user usage time data.

Usage data can also be obfuscated through RCA console. For more information, see the *Radia Client Automation Enterprise User Guide*.

## Handling Renamed Device

In Application Usage Manager, the Reporting Server provides all usage and inventory data report based on the name of a device. Whenever a device is renamed, the data about the device is stored twice in the database, with the old name and the new name. The Reporting Server treats the renamed device as a new device and gives information about both the devices.

For example, device A is renamed to device B, the Reporting Server treats device B as a new device and shows data associated with device A as well as with device B, which are same devices.

The Application Usage Manager uses the concept of Current Computer to avoid duplication of data. In the concept of Current Computer, the renamed device is treated as current or active device, and the data associated only with the current device is reported.

For more information, see ["Concept of Current Computer" on page 19](#).

During the first collection from the client device performed after renaming the device, the Usage Agent sends usage and inventory information with the both old and new device names. This occurs because the process of starting the operating system and renaming the device results in executables being launched under the old and the new names of the device.

After the first collection, you must update CurrentComputer column to 0 for the old device and then for subsequent collections, the Usage Agent sends the usage and inventory information of the renamed device only. The devices in the CurrentComputer column can be flagged to 0 or 1 using the Concept of Current Computer.

**Note:** On the client device, the `History.USDBase` file has both old and new device information. However, the history purge deletes the data whenever it qualifies for a history purge as scheduled.

## Internet Explorer Usage Counts for Windows Vista

When Internet Explorer is running on Windows Vista® (x64) with the Enable Protected Mode selected, (click **Tools > Internet Options > Security menu** to select Enable Protected Mode) each launch of the application results in usage count of two.

This is because when the user launches Internet Explorer, it first runs `IEUser.exe`, which runs at the default medium-integrity level. `IEUser.exe` then spawns a low-integrity level executable, `IEExplorer.exe`, which is the program the user sees and interacts with. Therefore, the usage count will always be two for each launch of Internet Explorer.

## Chapter 5

---

# Viewing Application Manager Usage Reports

This chapter describes various Application Usage Manager reports for current and non-current computers.

## Viewing Usage Reports

The Reporting Server provides web-based reports for Application Usage Manager.

To view the reports, access the **Reporting** tab in the RCA Console. Under Reporting Views, click **Usage Management Reports** to expand the list of reports.

**Caution:** For better performance, stop the RCA Knowledge Base Server before viewing usage reports from the Reporting Server.

**Note:** Reporting is optimized for display screen area setting 1024 x 768 or greater.

By default, the Reporting Server provides reports containing all current and non-current devices data. If required, you can generate the reports with data only for the current devices using the concept of Current Computer. For more information, see "[Concept of Current Computer](#)" on page 19.

## Usage Reports

There are different categories for Usage reports:

- Executive Summaries
- Top 10 Used Products Reports
- Operational Reports
- Device Reports
- Monthly Usage Reports
- Inventory Reports

Each of the above categories contains multiple reports.

## Executive Summaries

Executive Summaries report gives graphical representation of devices used to collect usage reports and also vendor and product usage report based on a month.

## Monthly Device Collection Statistics

Monthly Device Collection Statistics gives graphical representation of devices used to collect usage reports in the past one year with one data point for each month for past 12 months.

## Daily Device Collection Statistics

Daily Device Collection Statistics report gives graphical representation of devices used to collect usage reports in the past 30 days.

## Monthly Usage by Vendor

Monthly Usage by Vendor report gives the monthly usage summary information of the devices based on the vendor. This report includes information such as Vendor Name, Installed Devices, Usage Time, and Details.

## Monthly Usage by Product

Monthly Usage by Product report gives the monthly usage summary information of the device based on the product. This report includes information such as Product Name, Installed Devices, Usage Time, and Details.

## Top 10 Used Products Reports

Top 10 Used Products Reports give detailed information about top 10 application products used by the users as well as the system. This report is further categorized as For User Accounts and For Computer Accounts.

### For User Accounts - Total Usage Time

For User Accounts - Total Usage Time report gives detailed information about the top 10 application products used by the user accounts, such as administrator. This report includes information on Product Name and Usage Time.

You can filter each entry under Product Name column to view list of applications.

### For User Accounts - Total Focus Time

For User Accounts - Total Focus Time report gives detailed information about the top 10 application products used, based on the Focus Time.

### For User Accounts - Average Usage Per Day

For User Accounts - Average Usage Per Day report gives detailed information about the top 10 application products used, based on the average per day usage.

## **For User Accounts - Average Usage Per Day For User Accounts**

For User Accounts - Average Usage Per Day For User Accounts report gives detailed information about the top 10 application products used, based on the average per day usage.

## **For Computer Accounts - Total Usage Time**

For Computer Accounts - Total Usage Time report gives detailed information on the top 10 application products used by the computer accounts, such as system, local service, or network service. This report includes information on Product Name and Usage Time.

You can filter each entry under the Product Name column to view list of applications.

## **For Computer Accounts - Total Focus Time**

For Computer Accounts - Total Focus Time report gives detailed information on the top 10 application products used by the computer accounts, based on the Focus Time.

## **For Computer Accounts - Average Usage Per Day**

For Computer Accounts - Average Usage Per Day report gives detailed information about the top 10 application products, used through the computer accounts, based on the average per day usage.

## **For Computer Accounts - Average Usage Per Day For Computer Accounts**

For Computer Accounts - Average Usage Per Day For Computer Accounts report gives detailed information about the top 10 application products, used through the computer accounts, based on the average per day usage.

## **Operational Reports**

Operational Reports give database specific statistics as well as information of the devices in your network. You can view report details for three new reports namely, Device Collected, Device Not Collected, and Database Statistics.

### **Device Collected**

Device Collected report gives detailed information about all devices that were collected on yearly and monthly basis. When you select a particular year for which you want to generate the report, it gives you a detailed month wise summary. When you select a month, it gives you a detailed list of the devices collected in that month.



## Device Not Collected

Device Not Collected report gives detailed information about all the devices that were not collected in the past 30 days.

## Database Statistics

Database Statistics report gives detailed information about the current database statistics. This list is useful when records in certain tables grow very large.

## Device Reports

Device Reports give detailed applications usage information based on devices and users using the applications.

### Usage by Device

Usage by Device report gives detailed information on the devices in the network, such as Device Name, Domain Name, Users, Operating Systems, OS level, Product Usage, First Collection, and Last Collection.

You can filter each entry under Device, Operating System, and OS Level columns to view all details specific to the entry. For example, clicking **Show Product Usage** gives you Monthly Usage by Product report.

### Usage by User

Usage by User report gives detailed information of the users using the application installed.

You can filter each entry under the User Name column to view all details specific to the entry. For example, clicking **Show Product Usage** gives you Monthly Usage by Product Version report.

## Monthly Usage Reports

Monthly Usage Reports give detailed usage specific information based on vendors, product and applications for a month.

### Vendor Reports

Vendor Reports give detailed usage by vendor information.

### Monthly Usage by Vendor

Monthly Usage by Vendor report gives detailed information on Vendor, Installed, Used, Unused, Used percentage, Usage status, Usage time, and Focus time.

You can filter each entry in the Vendor column to view specific details. For example, clicking a vendor name in the Vendor column gives you Monthly Usage by Product report.

## Product Reports

Product Reports give detailed usage by product information.

### Monthly Usage by Product

Monthly Usage by Product report gives detailed information on Product Name, Installed, Used, Unused, Used percentage, Usage status, Usage time, and Focus time.

You can filter each entry in the Product Name column to view specific details. For example, clicking a product name in the Product Name column gives you Monthly Usage by Product Version report.

### Monthly Usage by Product Version

Monthly Usage by Product Version report gives detailed information on Product Name, Product Version, Installed, Used, Unused, Used percentage, Usage status, Usage time, and Focus time.

You can filter each entry in the Product Name and Product Version columns to view specific details. For example, clicking a product name in the Product Name gives you Monthly Usage by Application report.

## Application Reports

Application Reports give detailed information about the usage of the applications installed on the devices.

### Monthly Usage by Application

Monthly Usage by Application report gives detailed information on Application Name, Installed, Used, Unused, Used Percentage, Usage Status, Usage Time, and Focus Time.

You can filter each entry in the Application Name column to view specific details. For example, clicking an application name in the Application Name column gives you Monthly Usage by Application Version report.

### Monthly Usage by Application Version

Monthly Usage by Application Version report gives detailed information on Application Name, Application Version, Installed, Used, Unused, Used percentage, Usage Status, Usage Time, and Focus Time.

You can filter each entry in the Application Name and Application Version columns to view specific details. For example, clicking an application name in the Application Name column gives you Inventory by Application Signatures report.

## Inventory Reports

Inventory Reports give application specific statistics, such as the application installed in your network and details of the devices where applications have been installed. You can view the reports based on Application, Application Version, and Application Signature.

### Vendor Reports – Inventory by Vendor

Inventory by Vendor report gives reports based on Vendor, Installed Products, and Installed Devices.

You can filter each entry in the Vendor and Installed Devices columns. For example, clicking a vendor name in the Vendor column gives you Inventory by Product report.

### Product Reports

Product Reports give detailed inventory information based on Product and Product Versions.

### Inventory by Product

Inventory by Product report gives reports based on Product Name, Installed Applications, and Installed Devices.

You can filter each entry in the Product Name and Installed Devices columns. For example, clicking a product name in the Product Name column gives you Inventory by Product Version report.

### Inventory by Product Version

Inventory by Product Version report gives reports based on Product Name, Product Version, and Installed Devices.

You can filter each entry in the Product Name, Product Version, and Installed Devices columns. For example, clicking a product name in the Product Name column gives you Inventory by Application report.

### Inventory by Application

Inventory by Application report gives detailed information about the applications currently installed in your network.

You can filter each entry in the Application and Installed Devices columns. For example, clicking an application name in the Application column gives you Inventory by Application Version report.

## Inventory by Application Version

Inventory by Application Version report gives detailed information about the applications currently installed in your network. The report also shows the application version, description, and the number of the devices where the application is installed sorted by the application version.

You can filter each entry in the Application, Application Version, and Installed Devices columns. For example, clicking an application name in the Application column gives you Inventory by Application Signature report.

## Inventory by Application Signature

Inventory by Application Signature report gives detailed information about the applications currently installed based on their signature. You can view reports based on Application Name and Installed Devices.

You can filter details on Application Name and Installed Devices columns. For example, clicking an application name in the Application Name column, gives you a detailed report on Application Name, Application Version, Application Description, Size (bytes), Installed Devices, and MD5 Hash.

You can further filter each entry in the Installed Devices column. For example, clicking a device in the Installed Devices column, takes you to the Inventory by Application Signatures by Device report. Clicking a path in the Paths column gives you complete path details where the application is installed.

# Filtering Usage Management Reports with Reporting Server

Reporting Server provides extensive filtering capabilities. You can filter the reports displayed in the Reporting tab using the Data filters.

To access the data filters:

1. On the Core console, click **Reporting** tab.
2. Under **Search Options - Data Filters**, expand **Usage Management Filters**.
3. Expand each individual Usage Management Related Data Filter to refer to the available filters you can apply to the current Reporting View.

Filter types include:

- **Device Filters**  
These filters are used to filter reports based on the device properties, such as domain name, device name, and user name.
- **OS Filters**  
These filters are used to filter reports based on the Operating System and Operating System level of the devices.

- **Software Filters**  
These filters are used to filter reports based on the application properties, such as vendor name, product name, and product version.
- **Interval Filters**  
These filters are used to filter reports based on the interval specified as start date and end date. The interval filter filters the data based on application usage data. The start date filters the applications used from the specified start date. The end date filters the applications used till the specified end date.
- **Rules**  
These filters are used to filter reports based on the specific search criteria , rule, rule set, or rule set group. Use the Application Usage Manager Administrator to create criteria, rules, rule sets, and rule set groups as described in next section.

For more information on creating filters and using the Reporting Server in general, see the *Radia Client Automation Enterprise Reporting Server Reference Guide*.

## Chapter 6

---

# Using the Application Usage Manager Administrator

Use the Application Usage Manager Administrator to create specific search criteria to be implemented when you are generating your usage monitoring reports. Creating these criteria enable you to supplement the existing search options and create better reports based on your individual organization's requirements. Note that RCA Application Usage Manager Administrator is available as a separate installer and is not installed with RCA Application Usage Manager. For more information, see *Radia Client Automation Enterprise Installation and Upgrade Guide*.

## Accessing the Application Usage Manager Administrator

1. From the **Start** menu, go to **Radia Client Automation Application Usage Manager > Application Usage Manager Admin**.
2. Select the name of the DSN that you will use and type your User Name and Password in the text boxes provided.
3. Click **OK**.

The Application Usage Manager Admin consists of four tabs you can use to define criteria, rules, rule sets, and rule set groups.

## Application Usage Manager Admin Search Function

After selecting criteria, rule, rule set, or rule set group, click the **Search** button to preview your query results. Query results are displayed in a table at the bottom of the Application Usage Manager Admin window.

The search function can be used at any stage of the rule creation process.

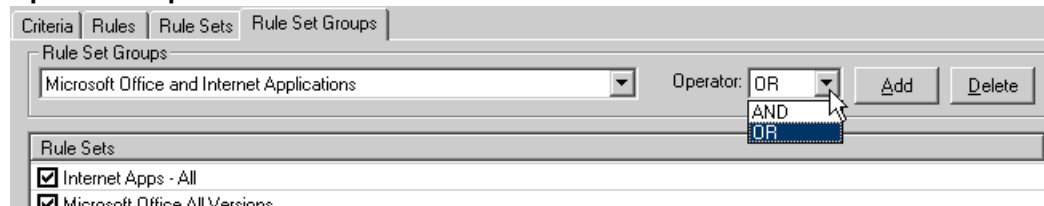
## Creating Criteria, Rules, Rule Sets, and Rule Set Groups

Use the Application Usage Manager Admin to create criteria, rules, rule sets, and rule set groups that are used to generate usage reports.

## Operators AND versus OR

There are two types of criteria, rules, rule sets, and rule set groups you can create: AND and OR. Before creating the rule, decide which type you would like to create and select the appropriate operator from the **OPERATOR** list.

### Operator drop-down list

The screenshot shows the 'Criteria' tab in the Application Usage Manager Administrator. The 'Rule Set Groups' section has a dropdown menu with 'Microsoft Office and Internet Applications' selected. To its right is an 'Operator' dropdown menu currently set to 'OR'. A mouse cursor is clicking on the 'AND' option in the dropdown. Below the 'Operator' dropdown are 'Add' and 'Delete' buttons. The 'Rule Sets' section below shows two checked items: 'Internet Apps - All' and 'Microsoft Office & All Versions'.

Creating a criterion using the AND operator specifies that in order for a record to match that criterion, all of the properties specified must be true. For example, a criterion designed with

Vendor Property	= Equals Microsoft
Application property	= Like WinWord
Operator	= AND

will return only Microsoft Word records.

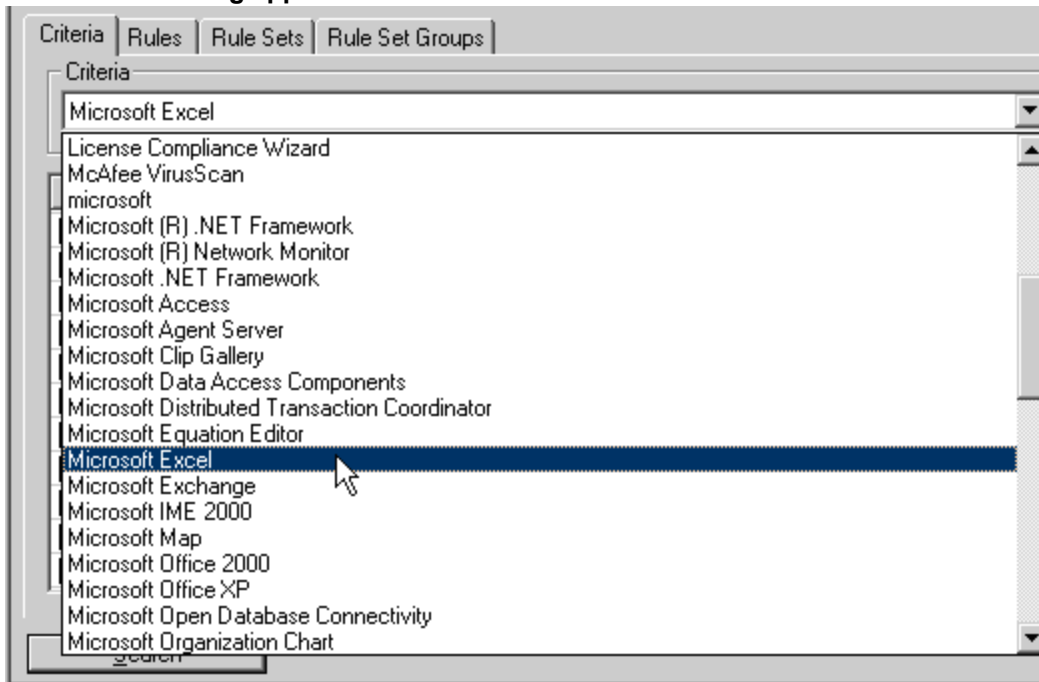
If the OR operator is selected in the above example, all applications with Vendor Microsoft are returned.

The AND operator is most effective when creating criteria only. The OR operator is more appropriate for creating rules, rule sets, and rule set groups.

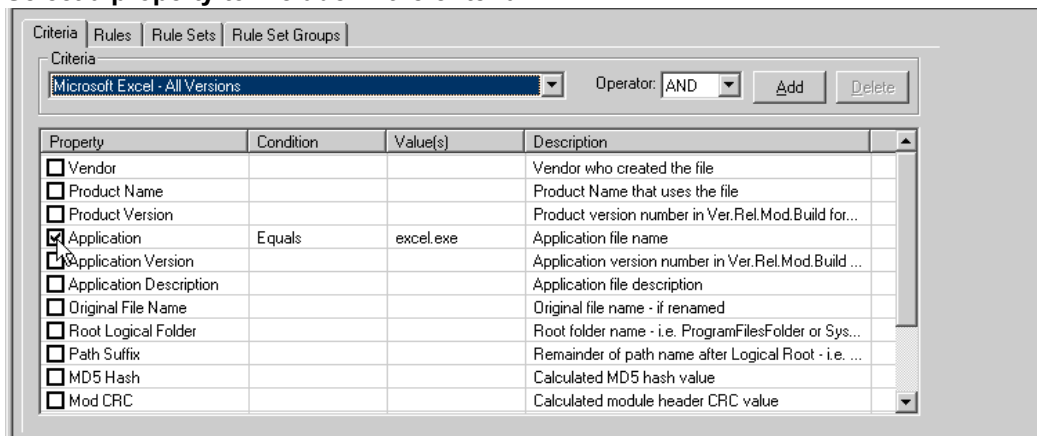
## Criteria Tab

Use the Criteria tab to define specific application criteria you use to display collected information when generating usage monitoring reports.

Before you select application criteria, use the Criteria list to check if any of the existing applications can be used.

**Choose an existing application to define criteria**

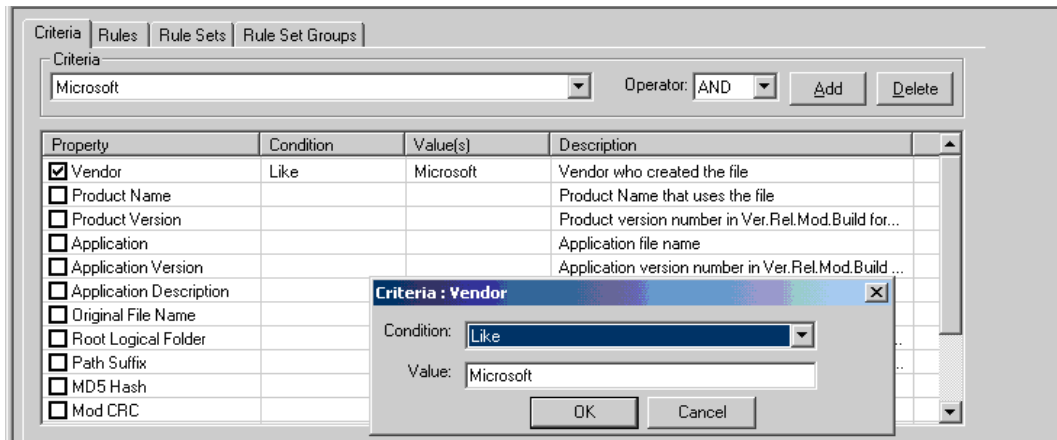
After you select an application from this list, select a **Property** check box to add that to the Criteria.

**Select a property to include in the criteria**

Double-click any row in the **Condition** or **Value** columns to add a condition and value to the criteria. As an example, the following steps describe how to create rule criteria where the Vendor property is equal to Microsoft.

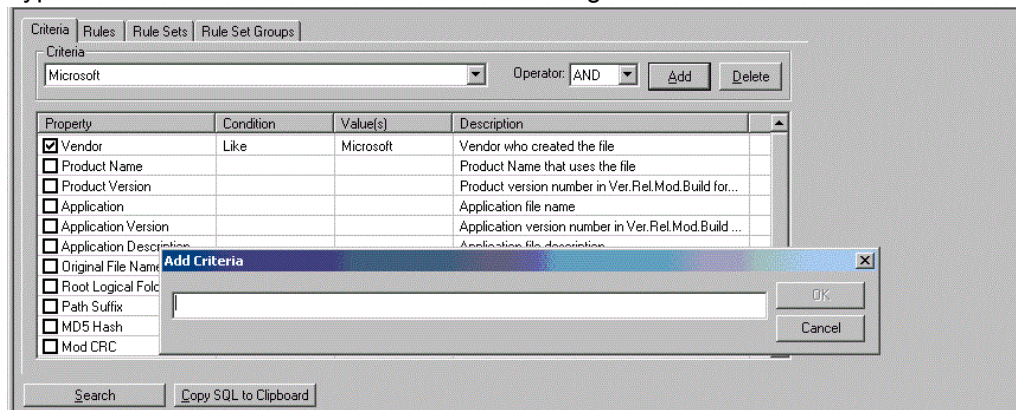


## Select a criteria condition and value



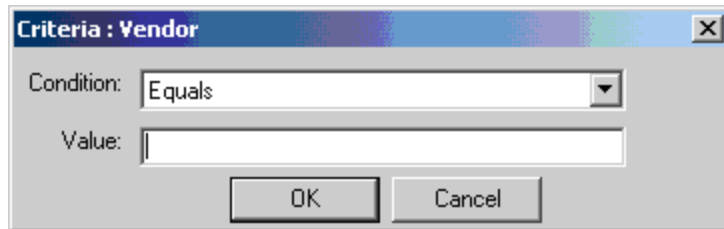
## Creating a criterion

1. To the right of the Criteria box, click the **Add** button to create new criteria. The Add Criteria dialog box opens.
2. Type a name for the criteria in the Add Criteria dialog box.



**Note:** Names are sorted in the report pages in ascending sequence. Therefore, frequently used names should be prefixed with a character that places them at the top of the sort sequence.

3. Click **OK** to close the Add Criteria dialog box.
4. Double-click the Vendor attribute row. The Criteria:Vendor dialog box opens.
5. Select **Equals** in the **Condition** list.
6. In the **Value** box, type **Microsoft**. Note that this value is used in a SQL command and must conform to SQL syntax rules.



Criteria : Vendor

Condition: Equals

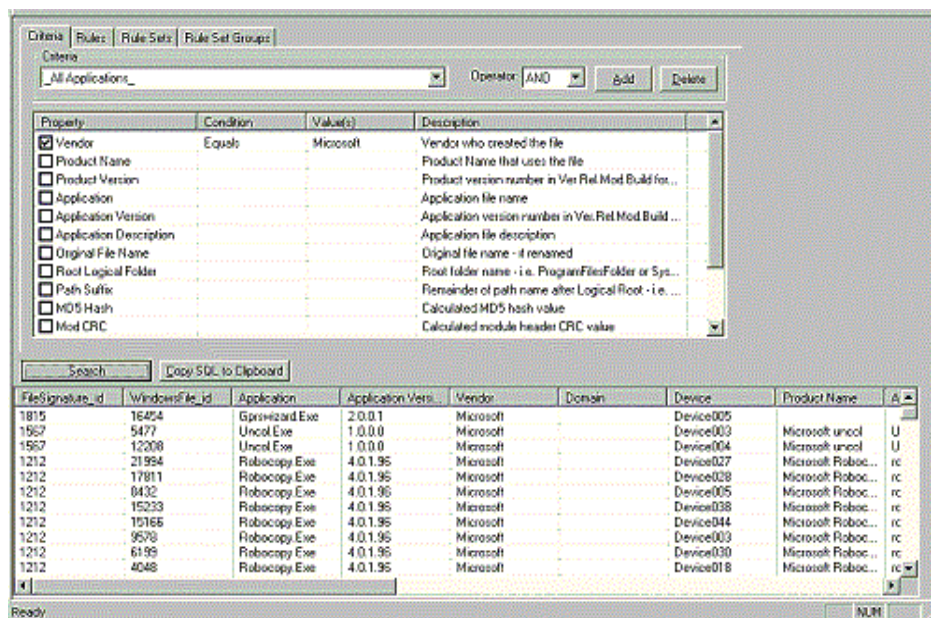
Value:

OK Cancel

**Note:** The typed text must conform to SQL Server query rules. For example, you can select the **LIKE** clause and type text such as %Microsoft% to define a criterion for any application whose Vendor definition contains the character string Microsoft.

**Note:** The use of LIKE clauses with preceding % may cause lengthy search times during reporting. It is recommended to use the EQUALS clause.

7. Test the criteria by clicking **Search** to retrieve all entries in the Application Usage Manager Knowledge Base that match the criteria you defined. Entries are displayed in the table at the bottom of the window.



Criteria : Vendor

Condition: Equals

Value: Microsoft

Search Copy SQL to Clipboard

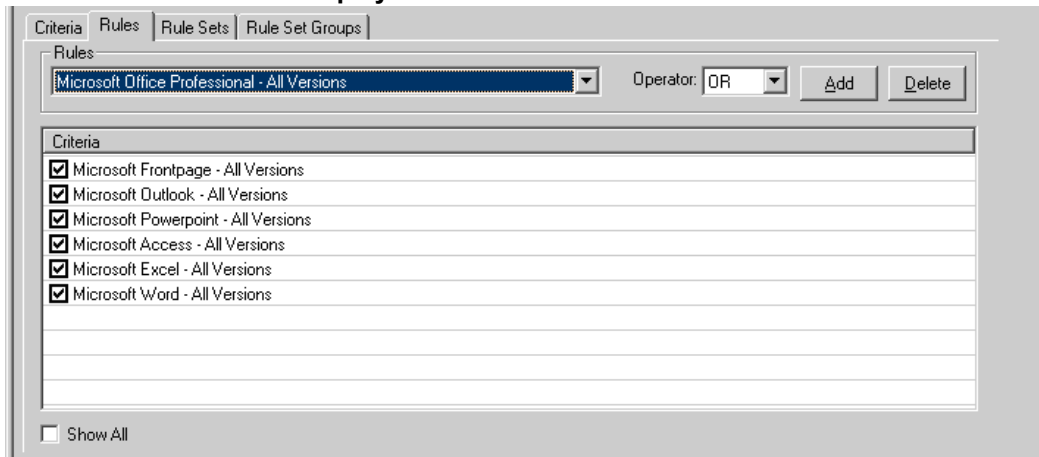
FileSignature_id	WindowsFile_id	Application	Application Vers.	Vendor	Domain	Device	Product Name	A
1815	16454	GpsWizard.exe	2.0.0.1	Microsoft		Device005	Microsoft uncol	U
1957	5477	Uncol.exe	1.0.0.0	Microsoft		Device003	Microsoft uncol	U
1957	12208	Uncol.exe	1.0.0.0	Microsoft		Device004	Microsoft uncol	U
1212	21994	Robocopy.exe	4.0.1.95	Microsoft		Device027	Microsoft Roboc...	rc
1212	17811	Robocopy.exe	4.0.1.95	Microsoft		Device028	Microsoft Roboc...	rc
1212	8432	Robocopy.exe	4.0.1.95	Microsoft		Device005	Microsoft Roboc...	rc
1212	15233	Robocopy.exe	4.0.1.95	Microsoft		Device038	Microsoft Roboc...	rc
1212	15165	Robocopy.exe	4.0.1.95	Microsoft		Device044	Microsoft Roboc...	rc
1212	9578	Robocopy.exe	4.0.1.95	Microsoft		Device003	Microsoft Roboc...	rc
1212	6199	Robocopy.exe	4.0.1.95	Microsoft		Device030	Microsoft Roboc...	rc
1212	4048	Robocopy.exe	4.0.1.95	Microsoft		Device018	Microsoft Roboc...	rc

The new criterion is complete and ready to be used in any rules you generate.

## Rules Tab

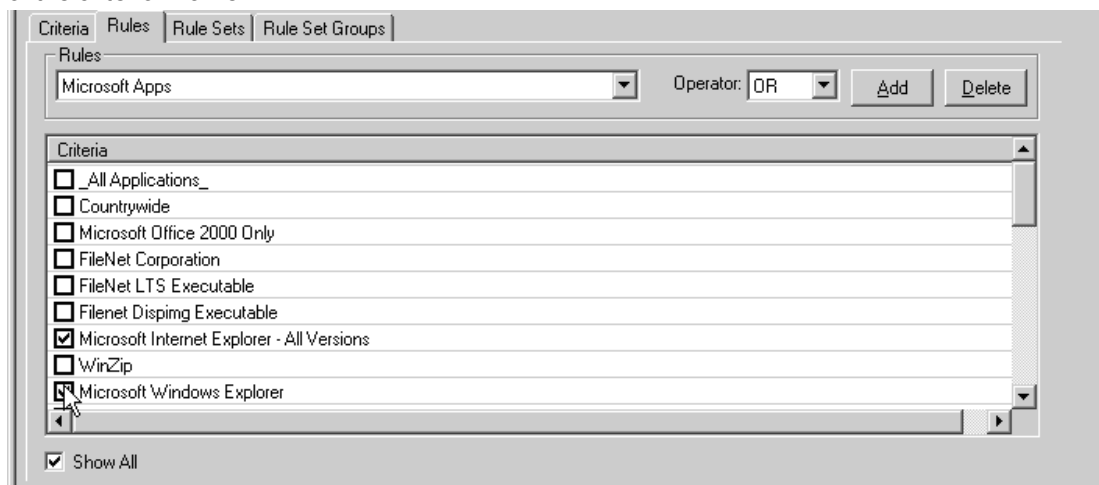
Rules are a combination of Criteria. Use the Rules tab to define rules based on the criteria you selected in the Criteria tab.

Use the Rules list to select any default rules. After a rule is selected, the criteria that are part of that rule are displayed.

**Criteria for each rule is displayed**

## Creating a new Rule

1. Click **Add** to define a new rule. The Add Rule dialog box opens.
2. Type a name for the rule in the **Add Rule** dialog box.
3. Click **OK**.
4. Select any criteria you would like to include in the new rule by clicking the check box to the left of the criterion name.



5. Test the rule by clicking **Search**. All matching records are displayed in the table at the bottom of the window.

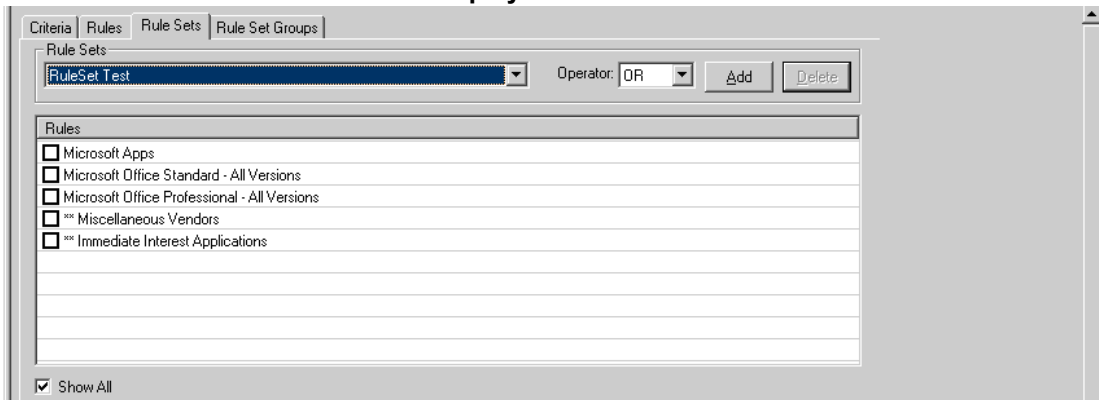
The new rule is complete and ready for inclusion in any Rule Sets you generate.

## Rule Sets Tab

A Rule Set is a grouping of Rules. Use the Rule Sets tab to define which rules you would like to combine to form a Rule Set instance.

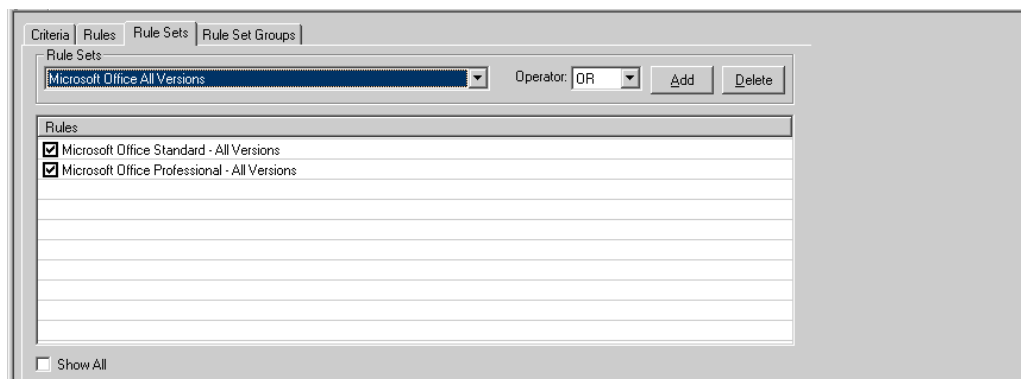
Use the Rule Sets list to select any existing Rule Sets. After a Rule Set is selected, the rules that make up that Rule Set are displayed.

Rules included in the Rule Set are displayed.



## Creating a new Rule Set

1. Click **Add** to define a new Rule Set. The Add Rule Set dialog box opens.
2. Type a name for the Rule Set in the **Add Rule Set** dialog box.
3. Click **OK**.
4. Select any rules you would like to include in the new Rule Set by clicking the check box to the left of the rule name.



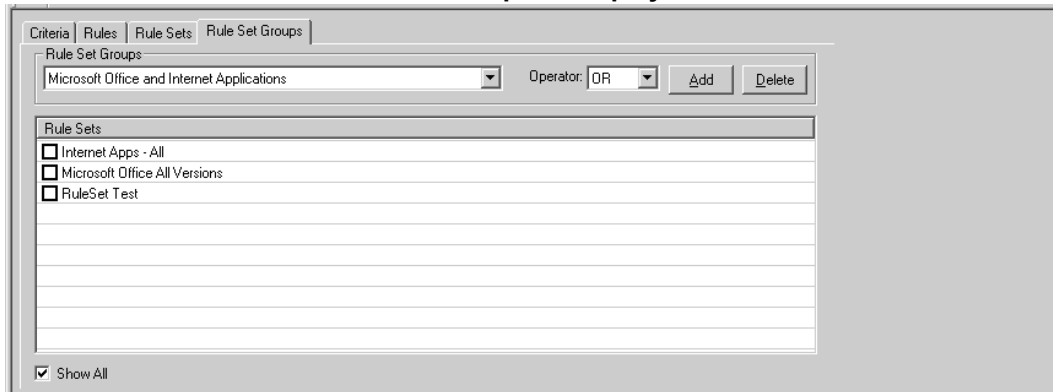
5. Test the Rule Set by clicking **Search**. All matching records are displayed in the table at the bottom of the Application Usage Manager Admin window.

The new Rule Set is complete and ready for inclusion in any Rule Set Groups you may generate.

## Rule Set Groups Tab

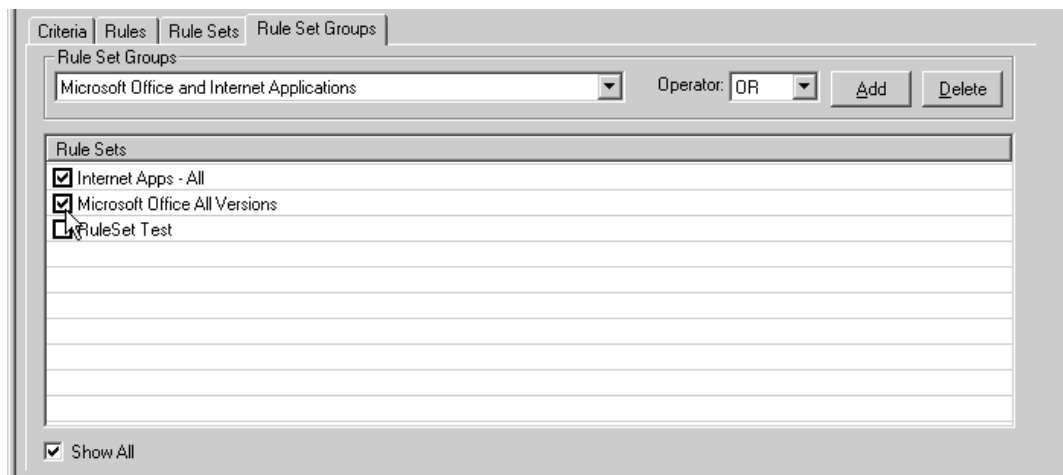
If you want to combine multiple Rule Sets, create a Rule Set Group instance.

Use the Rule Set Groups list to select any existing Rule Set Groups. After a Rule Set Group is selected, all of the Rules Sets that make up that Rule Set Group are displayed.

**Rule Sets included in the Rule Set Group are displayed**

## Creating a new Rule Set Group

1. Click **Add** to define a new Rule Set Group. The Add Rule Set dialog box opens.
2. Type a name for the Rule Set Group in the **Add Rule Set** dialog box.
3. Click **OK**.
4. Select any Rule Sets you would like to include in the new Rule Set Group by clicking the check box to the left of the Rule Set name.



5. Test the Rule Set Group by clicking **Search**. All matching records are displayed in the table at the bottom of the Application Usage Manager Admin window.

The new Rule Set Group is complete.

Now that you have finished creating criteria, rules, rule sets, and rule set groups, you can generate reports based on your own specifications using the report generator options Include Rule and Exclude Rule. For more information, see ["Viewing Usage Reports" on page 46](#).

## We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click [here](#).

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to [radiadocfeedback@persistent.co.in](mailto:radiadocfeedback@persistent.co.in).

**Product name and version:** Radia Client Automation Enterprise Application Usage Manager, 9.00

**Document title:** Reference Guide

**Feedback:**

